Examining Leading Pakistani Mobile Apps

Sana Habib
Arizona State University
shabib3@asu.edu

Mohammad Taha Khan
Washington and Lee University
tkhan@wlu.edu

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

ABSTRACT

In this paper, we explore the security and privacy concerns associated with a small group of widely used Pakistani mobile apps that tens of millions of Pakistanis depend on for essential services. Using both static and dynamic analysis techniques, we evaluated each app in three critical areas: (i) the volume of personal data collected, its management, and the risk of exposure; (ii) vulnerabilities in password and login security; and (iii) network security, with a focus on threats from compromised server keys. These issues are significant for at-risk users, such as journalists, activists, media professionals, and victims of domestic abuse, who face increased threats of surveillance and targeted attacks in the region. In Pakistan, censorship frequently involves acquiring user credentials to facilitate monitoring and intimidation of at-risk users, often accompanied by threats of violence. Importantly, it is not only government actors who possess the resources and power to enforce such censorship; private entities, including criminal organizations and domestic abusers, can also engage in similar tactics. Consequently, the security and privacy concerns that we address are crucial not only for the protection of journalists and activists but also for the protection of victims of domestic abuse throughout the region.

KEYWORDS

Excessive and Exposed Personally Identifiable Information (PII), Android Memory Forensics, Missing Password, Pakistan.

1 INTRODUCTION

With support from a non-profit digital rights foundation in Pakistan, we identified seven popular mobile apps (given in Table 1) used daily by tens of millions of Pakistanis. These apps fall into two categories: government-developed apps and telco apps. We selected them because users are motivated to download and retain them for various reasons, such as access to government services, promotional offers, and their user-friendly design. Given these solid incentives for user engagement, these apps are particularly relevant to our study.[1] For example, the Pak Identity [61] app allows users to request, update, and modify identity documents without visiting the NAtional Database and Registration Authority (NADRA) office. The Pakistan Citizen Portal [62] app allows citizens to file complaints against corrupt officials. The Qeemat Punjab [39] app tracks agricultural prices and identifies corrupt agribusinesses. The four leading telco apps allow downloading tax certificates, eliminating the need for office visits. Since tens of millions of Pakistanis rely on these apps, we aimed to investigate their security and privacy conditions to ensure that users are protected from potential threats. The seven apps we examined can be categorized as follows.

- Government Apps: Pak Identity [61], Pakistan Citizen Portal [62], Qeemat Punjab [39].
- Telco Apps: SIMOSA [68], My Zong [59], My Telenor [58], UPTCL [71].

Among the seven apps we analyzed, we identified significant security and privacy issues related to PII's excessive collection, storage, and management. All three government apps collect location coordinates—unnecessary data for their core functionality—and store user credentials in plaintext in the root directory of the Android file system. In Pakistan, where device confiscation by law enforcement (with or without a warrant) is common and where private attackers or domestic abusers may also steal or gain access to devices, this presents a serious security risk. Storing user credentials in plaintext makes it relatively easy for attackers to exfiltrate this sensitive information. Moreover, the app developers do not disclose in privacy policies and user agreements the storage of user credentials in plaintext in the Android file system. We also found login security gaps across all the apps. In response, we have sent ethical disclosure emails to the app vendors and are following up. Specifically, we found the following issues:

- All three government apps collect excessive PII, including location coordinates, which are unnecessary for their functionality.
- Six of the seven apps analyzed store user credentials in plaintext in the root directory of the Android file system.
- All four telco apps have a password vulnerability that could expose user credentials in case of a confiscated, stolen, compromised, or shared device.
- All seven apps have login security gaps that allow access from unknown devices and locations without notifying the user.
- Despite using TLS encryption, all three government apps and two telco apps are vulnerable to in-path attacks if a server's private key is compromised, enabling adversaries to decrypt data, steal credentials, and even plant false evidence (in case of government apps)—a risk heightened in Pakistan by potential corruption among government officials [3, 22, 27, 63].

2 MOTIVATION

Press freedom and the safety of journalists and activists in Pakistan have significantly deteriorated in recent years [23, 67]. Several incidents highlight this decline, including May 9, 2023, riots [30, 54]

[1] The detailed app selection criteria are given in Appx. A purely to save space.

Free and Open Communications on the Internet 2025(1), 24–41

Table 1: Mobile Apps analyzed during project.

	App Title	Developer	Use	Popularity
1.	Pak Identity [61]	National IT Board, Government of Pakistan.	Request, Modify, and Update National Identity Documents.	Over one million downloads on Google Play Store [61].
2.	Pakistan Citizen Portal [62]	National IT Board, Government of Pakistan.	Grievance Redressal System.	Over five million downloads on Google Play Store [62].
3.	Qeemat Punjab [39]	Punjab IT Board, Provincial Government of Punjab.	Get awareness regarding daily prices of agriproducts.	Over one million downloads on Google Play Store [39].
4.	SIMOSA (Previously Jazz World) [68]	Pakistan Mobile Communications Limited (doing business as Jazz).	Manage your Jazz mobile plan.	Holds a market share of 37% with ≈ 71 million subscribers [55] and over fifty million downloads on Google Play Store [56].
5.	My Zong [59]	CMPak Limited.	Manage your Zong mobile plan.	Holds a market share of 21% with ≈ 49.67 million subscribers and over fifty million downloads on Google Play Store [56].
6.	My Telenor [58]	Telenor Pakistan.	A one stop solution to all Telenor mobile number related needs.	Holds a market share of 20% with ≈ 44.14 million subscribers and over fifty million downloads on Google Play Store [56].
7.	UPTCL [71]	Pakistan Telecommunication Mobile Limited.	Manage your UPTCL mobile plan.	Holds a market share of 11% with ≈ 26 million subscribers and over ten million downloads on Google Play Store [56].

and February 8, 2024, elections [60], during which local police arrested journalists (who were carrying out their work-related duties) and confiscated their devices. Law enforcement justified these actions by citing location data and geo-fencing techniques, claiming they were necessary to maintain public order.

The broader threat to journalists' safety in Pakistan has been longstanding. In 2020, the country ranked ninth on the Committee to Protect Journalists' Global Impunity Index, with at least fifteen unsolved murders of journalists since 2010 [5]. Two tragic incidents in 2021 underscore this risk: Shahid Zehri, a local reporter, was killed in a car bombing in Balochistan [15], and Muhammad Zada Agra, a journalist critical of local police inaction regarding drug cartels, was shot near his home [11]. Both cases remain unresolved, with the perpetrators still unidentified.

The violence against journalists continued in 2021, exemplified by the attack on Asad Ali Toor, who was assaulted in his home by three men, likely in retaliation for his outspoken criticism of Pakistan's military [16]. Similarly, senior journalist Absar Alam was shot near his home, though he survived the attack. In 2024, a leaked audio recording revealed threats against Alam, further exposing the efforts to coerce him into issuing media licenses under duress [8]. The risks faced by reporters were starkly highlighted again in 2023 with the abduction of journalist Gohar Wazir [41]. More recently, Pakistan authorities prevented Baluch activist Mahrang Baloch from leaving Pakistan to attend a U.S. event, with no legal or valid justification provided for her detention [65].

In addition to physical threats, Pakistan's increasing reliance on surveillance technologies has raised significant concerns. Reports from 2021 highlighted Israeli surveillance technology despite the lack of formal diplomatic relations between the two countries [14]. These developments underscore the growing role of geolocation data in targeting at-risk individuals, particularly journalists. While authorities can use Israeli technology to extract user credentials and track individuals, locally developed apps provide a more accessible and cost-effective means of surveillance. That further emphasizes the urgent need to address the security and privacy risks posed by Pakistan's leading mobile apps.

In addition to threats against journalists, Pakistan faces pervasive domestic violence, including physical and psychological abuse [77]. Abusers often exploit victims' phones to monitor communications and exert control. As discussed later in this paper, weaknesses in telecommunications apps, such as inadequate password protections, allow abusers to retrieve call and SMS histories even after app deletion. The 2023 Mobile Gender Gap Report by GSMA [31] reveals Pakistan's significant gender gap in mobile usage and ownership, with women far more likely than men to rely on shared devices. This reliance further exposes female victims to digital vulnerabilities, enabling abusers to reclaim deleted data via telco apps.

The low standards for software development in the country exacerbate these security concerns. In 2023, reports of data leaks from NADRA mirrored earlier breaches involving biometric data in 2021 [12, 32]. In addition, millions of personal records were exposed online in 2023 due to software vulnerabilities [25, 28]. The 2021 Bykea app breach [9] and the 2020 Netwalker ransomware attack [6] further revealed critical security gaps. These incidents highlight the need to thoroughly examine leading Pakistani mobile apps—especially state-sponsored apps that collect unnecessary user credentials and telco apps that store sensitive call and SMS histories—to understand the significant security risks they pose to Pakistani users.

3 ETHICS

All seven apps listed in Table 3 are publicly available on Google Play Store [53] and APK Pure [47]. Our goal was to thoroughly assess the surveillance risks and potential for targeted attacks associated with these apps while adhering to ethical standards and ensuring

Table 2: Example Attacker Profiles. (Keys: Red –> State Attacker, Blue –> Non-State Attacker, Pink –> Hybrid Attacker.)

	Access to Server Private Key	Device Compromise			In-path Network Manipulation	Coerced Credential Retrieval (Server)
		Confiscation	Stealth	Usurpation		
Local Law Enforcement	✓	✓	×	×	✓	✓
Criminal Group	×	×	✓	×	×	×
(Tech-Savvy) Domestic Abuser	×	×	×	✓	✓	×
Corrupt Local Police Officer	✓	✓	×	×	✓	✓
Coerced or Compromised ISPs	✓	×	×	×	✓	×

Table 3: Ethical Disclosure Timeline.

	App Title	Email/Complaint Date
1.	Pak Identity [61]	Mar 14, 2024; Apr 13, 2024
2.	Pakistan Citizen Portal [62]	Mar 14, 2024; Apr 09, 2024
3.	Qeemat Punjab [39]	Mar 14, 2024; Apr 13, 2024
4.	SIMOSA [68]	June 24, 2024
5.	My Zong [59]	Nov 03, 2024
6.	My Telenor [58]	Nov 04, 2024
7.	UPTCL [71]	July 30, 2024

no violations occurred. To achieve this, we sent ethical disclosure emails to the app developers outlining the security and privacy concerns we identified in each app. Table 3 shows the timeline for these disclosures.

We first contacted the developers of all three government apps via email. After receiving no response, we followed up by submitting complaints through the Pak Identity [61], Pakistan Citizen Portal [62], and Qeemat Punjab [39] apps. We received an acknowledgment from the Pak Identity developers regarding the excessive collection of PII, including location coordinates, and they stated that they value our feedback. We also notified the developers of all four telco apps about a critical issue: the missing password functionality. While we have yet to receive a response from the developers of SIMOSA [68] and UPTCL [71] apps, we did receive acknowledgments from the developers of My Zong [59] and My Telenor [58] apps. However, whether these acknowledgments indicate a commitment to address the identified issues remains to be determined. For those developers who acknowledged our disclosure, we informed them of our 45-day ethical disclosure process, after which we plan to make our findings public if developers do not address the issues.

4 ATTACKER PROFILES

This section overviews the attackers' types, capabilities, and goals. The example attacker profiles, summarized in Table 2, are based on the local situation in Pakistan.

4.1 Attacker Types and Goals

Pakistan has three broad categories of attackers: state, private, and hybrid.

4.1.1 State Attacker. The first type of attacker is state actors, which includes local law enforcement agencies seeking to obtain sensitive user credentials such as full name, mobile number, call history, and SMS history to track and monitor activities or plant fake evidence (e.g., spoofing location data). Local law enforcement encompasses local police, district police, and specialized units such as the Federal Investigation Agency (FIA) anti-terrorism wing [2]. As shown in Table 2, local law enforcement can access the server's private key, enabling them to view app traffic in plaintext and potentially eavesdrop, intercept, or manipulate it. Additionally, they may confiscate a user's device and forcefully extract user credentials from the app server.

4.1.2 Private Attacker. The second type of attacker consists of private individuals, including members of criminal organizations, religious cults, drug traffickers, and groups involved in faith-based violence, as well as domestic abusers. These attackers have two primary capabilities: they can steal or seize a device, and they may manipulate network traffic if they control local network infrastructure. Table 2 outlines the capabilities of two private attacker profiles: those from criminal groups and domestic abusers.

4.1.3 Hybrid Attacker. The third type of attacker includes corrupt individuals within government organizations and those who can be influenced or coerced by corrupt actors, such as an Internet Service Provider (ISP). For instance, private attackers may bribe these insiders to exploit their positions and leak personal information about at-risk users. Corrupt government officials might also bribe an ISP to manipulate location data for political purposes. Table 2 outlines profiles of a corrupt local police officer who could leak user credentials and an ISP capable of eavesdropping, intercepting, and manipulating network traffic to plant fake evidence.

Attacker Goals. All three types of attackers aim to gain access to sensitive information about the victim, including location coordinates, mobile numbers, call history, SMS history, or any other data that would allow them to spy on, track, and monitor an at-risk individual.

4.2 Attacker Capabilities

The three types of attackers can have the following capabilities.

4.2.1 Physical Device Compromise. All three attacker types can compromise the physical device. For example, state actors may confiscate devices, while private attackers typically steal them. Hybrid attackers can engage in both actions. Additionally, domestic abusers can forcibly acquire the device, either with or without the victim's consent and knowledge. We assume that when the device is confiscated, stolen, or usurped, it does not contain any PII (such as call history, SMS history, personal documents on SD card, or photos); it only includes a leading Pakistani mobile app.

4.2.2 In-path Network Position. An in-path network position with access to the server's private key allows attackers to view data in plaintext, enabling them to monitor at-risk users' activities and extract sensitive information, such as emails and passwords. Additionally, the attacker can intercept and modify data in real time to fabricate evidence and frame the user. Both state-sponsored and hybrid attackers are capable of exploiting this vulnerability. Furthermore, private attackers who control local network infrastructure—such as a home router—can manipulate traffic to exploit the victim further, amplifying the potential for harm.

5 THREAT CLASSIFICATION

During our analysis, we used a Motorola Moto G7 Plus[2] device to dynamically test each app's behavior. We focused exclusively on Android for this study (rather than iOS or other platforms) since Android dominates the market in Pakistan, holding 95.26% of the market share [57]. Given the local context in Pakistan, where censorship often involves acquiring user credentials via device confiscation, intercepting network traffic, and planting false evidence to arrest at-risk individuals, we assessed each app based on three key security and privacy threats:

(1) Unnecessary Disclosure – This refers to collecting unnecessary personal data, transmitting that data without explicit consent in the privacy policy, and storing data in plaintext within the device's file system. Such practices increase the risk of data theft or exfiltration, especially if the device is confiscated or stolen (elaboration in Appx. B.1).

(2) Login Weaknesses – These vulnerabilities occur when apps lack user passwords, exposing data if the device is stolen or confiscated. Additionally, when apps fail to detect or alert users about logins from unknown devices, attackers can access accounts without the user's knowledge. (elaboration in Appx. B.2).

(3) Network Security Threats – This refers to unencrypted, cleartext traffic, which makes data vulnerable to interception. In Pakistan, with a high corruption index [33], we also explored the risks of compromised server private keys, enabling attackers to eavesdrop on sensitive credentials and inject false data, undermining user information security (elaboration in Appx. B.3). While a compromised server private key is a threat in any context, the political and social context in Pakistan is different, highlighting that solutions such as TLS and certificate pinning do not fully address the needs of at-risk Pakistani users.

6 APP CLASSIFICATION

This section provides background on the government and telco apps we analyze.

6.1 Government Apps – Pak Identity, Citizens Portal, Qeemat Punjab

The first set of apps we analyzed included widely used apps developed by the government of Pakistan. The federal government creates two apps; the third is from a provincial authority. The federal apps—Pak Identity (pk.gov.nadra.pakid) and Citizens Portal Pakistan (com.govpk. citizensportal)—are marked with "pk.gov" and "govpk" in their package names, signifying their official government affiliation. In contrast, the Qeemat Punjab app, developed by the Punjab Information Technology Board (PITB), features "pitb" in its package name, highlighting its provincial origin. This distinction underscores the collaborative efforts between federal and provincial governments to provide essential services to citizens.

The Pak Identity app [61], developed by the NADRA, facilitates the process of requesting, updating, and modifying national identity documents, including the Computerized National Identity Card (CNIC), National Identity Card for Overseas Pakistanis (NICOP), and Pakistan Origin Card (POC). NADRA, which manages the sensitive database of all Pakistani citizens, allows users to take and upload photos, undergo biometric verification, and make payments for various services via the Pak Identity app. Users create accounts using their email ID and password, and the app requires the location coordinates of users to provide the desired service.

The Citizens Portal app [62] acts as a grievance redressal system, enabling citizens to file complaints about federal and local government departments. Users create accounts using their CNIC and password; the app requires location coordinates when submitting complaints. This app serves as an essential tool for enhancing government accountability.

The Qeemat Punjab app [39], developed by the Punjab IT Board, is designed to inform the public about the daily prices of agricultural products set by Deputy Commissioners in Punjab, the country's second-largest and most densely populated province. Users who observe price discrepancies can submit complaints directly through the app to the relevant Price Control Magistrates; location permissions are required to submit a complaint.

6.2 Telco Apps – SIMOSA, UPTCL, My Zong, My Telenor

The second group of apps analyzed in this project includes client apps from significant telco operators in Pakistan: SIMOSA [68], My Zong [59], My Telenor [56], and UPTCL [71]. These apps help users efficiently manage their mobile services and account settings. Users can check their account balances, monitor usage, recharge their accounts, and access various services and promotions. Additional features include managing subscriptions, purchasing data or voice packages, and receiving customer support. The apps store call history, SMS records, and tax certificates for a specified duration, as Table 4 outlines.

The SIMOSA [68] app, formerly Jazz World, is provided by Jazz, Pakistan's largest mobile network and Internet Services Provider (ISP), which has a market share of 37% with approximately 71 million subscribers [55]. The SIMOSA app boasts over 50 million downloads and is rated 4.5 out of 5 on the Google Play Store. CM-Pak Limited, operating as Zong, is Pakistan's second-largest mobile

[2] The identified vulnerabilities are intrinsic to the apps, independent of the Android version. We initially used Android 10.0 for testing because it introduced enhanced privacy controls and scoped storage. With a market share ≈ 7% in Pakistan [46], Android 10.0 is relevant, mainly because victims of domestic abuse can still rely on older versions, including Android 10.0 and earlier. We repeated the experiments with Android 15.0 and obtained the same results.

network operator, owned by China Mobile, with 49.67 million subscribers [73]. The My Zong app is rated 4.3 stars on the Google Play Store. Telenor is Pakistan's third-largest mobile network operator. Its app, My Telenor [58], is rated 4.2 stars. Ufone, launched by the Pakistan Telecommunication Company Limited (PTCL) in 2000, is currently owned 62% by the Government of Pakistan, 26% by a private group, and 12% by the general public. The UPTCL [71] app, provided by Ufone, has more than 10 million downloads and a rating of 4.3 stars on the Google Play Store.

7 METHODOLOGY

This section describes the test environment for evaluating each app against the three identified security threats. To ensure we were analyzing the official versions of the local apps, we manually downloaded the latest versions from the Google Play Store and installed them on the test device. We then extracted the APK files using the APK Extractor app [24] and transferred these files from the test device to our laptop via adb shell [45] for reviewing the app's source code.

For our experiments, we used a Motorola Moto G7 Plus with root access to install custom root certificates, enabling us to decrypt outgoing app traffic. A custom certificate generated by mitmproxy was installed on the device, allowing us to intercept the app's traffic for analysis, including examining the transmitted data and its destinations. We ran the mitmproxy on an Ubuntu 22.04 laptop. To bypass security measures such as root detection and SSL pinning, we used Frida scripts [70]. Over twelve months, we periodically interacted with each app for several minutes, engaging with key features such as navigating main pages, exploring tabs, filing complaints, making requests, viewing call and SMS history, and downloading tax certificates (where applicable) to generate traffic. That enabled us to observe whether the app used TLS encryption, analyze the data types transmitted, and examine the possibility of network manipulation.

7.1 Unnecessary Disclosure

We manually installed each app on the test device and created the necessary user accounts. We first reviewed the personal data required during registration to detect excessive PII and determine whether it was essential for the app's core functionality. After logging into each app, we generated app traffic. We examined the files created within the app's installed package, specifically focusing on identifying any PII stored in plaintext within the root directory of the Android File System.

To identify disclosed PII, we conducted a dynamic analysis using mitmproxy on a rooted device to decrypt the app's outgoing HTTPS traffic. That allowed us to capture and inspect the encrypted traffic in real-time, enabling us to detect whether any PII was being transmitted. During this analysis, we manually reviewed each request in mitmproxy, carefully examining the data packets for any PII being shared without proper disclosure in the app's privacy policy. To ensure the accuracy of our findings, we repeated the experiment—closing and reopening the app—to verify the consistency of any identified PII leaks.

7.2 Login Weaknesses

This step involves manually logging into each app to check for the absence of a user password feature. To test for missing detection of unknown login activity, we installed the app on a research team member's phone (the actual user), logged into the app, and generated some traffic. Then, we installed the app on a test device and logged in using the research team member's credentials. If the app does not trigger a notification or warning on the original device about the new login, the app lacks the feature to detect unauthorized login attempts.

7.3 Network Security Threats

We used PCAPdroid [64] to capture the traffic exchanged between each app and its server to assess network security vulnerabilities. We analyzed this traffic in Wireshark [72], explicitly searching for an HTTP response code of 302, which could indicate a potential SSL stripping attack [43]. We conducted a dynamic analysis using a mitm proxy to analyze the data spoofing vulnerability. We intercepted meaningful requests, such as the ones sending location coordinates to the server and the ones from the server sending PDF documents to the user's device. We concluded that data spoofing was possible if the response was sent to the server or the device without errors.

8 RESULTS

In this section, we present the findings from our analysis of the government and telco apps, summarizing the results provided in Table 4.

8.1 Government Apps – Pak Identity, Citizens Portal, Qeemat Punjab

All three government apps require location permissions to function. For instance, the Pak Identity app [61] cannot be used unless the user grants location permissions. Similarly, the Pakistan Citizen Portal [62] and Qeemat Punjab [39] apps require location access to submit complaints. However, the need for location data raises concerns, as these apps collect excessive PII that seems unnecessary for their core functionality.

For example, the Pak Identity app, which is designed for updating national identity documents, transmits location coordinates every time the user logs in (Fig. 1a, Appx. C). This data is not required for the app's primary purpose. The Pakistan Citizen Portal app, which is intended for grievance redressal, asks users to provide detailed personal information, such as religion, blood group, date of birth, and physical address—data that should not be necessary for filing a complaint (Fig. 5, Appx. D). Furthermore, the app requires location permission to submit a complaint (Fig. 8, Appx. D), and even includes a "hide my identity" feature, which, however, fails to function when submitting a complaint. Similarly, the Qeemat Punjab app requires users to provide their full name, profession, citizen ID, gender, and location before submitting a complaint, which further compromises user privacy (Fig. 10, 11, Appx. E). This extensive data collection makes it easier for state actors to track and monitor claimants.

In addition to excessive data collection, all three apps store sensitive information in plaintext in the root directory of the Android

Table 4: Assessment Results of Pakistani Mobile Apps.

Embedded Certificates within App Packages.

	App Title	Root Detection	SSL Pinning	Embedded Certificates (directory inside app package)
1.	Pak Identity [61]	×	✓	–
2.	Pakistan Citizen Portal [62]	×	✓	res/raw/pmdu_gov _pk.crt
3.	Qeemat Punjab [39]	×	✓	–
4.	SIMOSA [68]	×	✓	assets/jazz_cert.crt, assets/new_cert.der
5.	My Zong [59]	×	✓	assets/golootlo_key_prod.pem, assets/zong-staging-public-key.pem
6.	My Telenor [58]	×	✓	assets/cbg_root. cer, res/GX.pem
7.	UPTCL [71]	✓	✓	–

Security and Privacy issues in Leading Pakistani Mobile Apps.
(Key: ♦ –> State Attackers, ▲ –> Private Attackers, ■ –>Hybrid Attackers, ♦̆ ▲̆ ■̆ –> Respective Attackers can Eavesdrop.)

	App Title	Unnecessary Disclosure		Login Weaknesses		Network Security Threats	
		Excessive PII	Exposed PII	Missing Password	Missing Login Detection	Missing TLS	Eavesdrop and Modify
1.	Pak Identity [61]	♦ ▲ ■	♦ ▲ ■	×	♦ ▲ ■	×	♦ ▲ ■ (Fig. 1,3, Appx. C)
2.	Pakistan Citizen Portal [62]	♦ ▲ ■	♦ ▲ ■	×	♦ ▲ ■	×	♦ ▲ ■ (Fig. 9, Appx. D)
3.	Qeemat Punjab [39]	♦ ▲ ■	♦ ▲ ■	×	♦ ▲ ■	×	♦ ▲ ■ (Fig. 12,13, Appx. E)
4.	SIMOSA [68]	×	♦ ▲ ■	♦ ▲ ■	♦ ▲ ■	×	|
5.	My Zong [59]	×	♦ ▲ ■	♦ ▲ ■	♦ ▲ ■	×	♦̆ ▲̆ ■̆ (Fig. 20, 21, Appx. G)
6.	My Telenor [58]	×	♦ ▲ ■	♦ ▲ ■	♦ ▲ ■	×	♦̆ ▲̆ ■̆ (Fig. 26, 27, 28, Appx. H)
7.	UPTCL [71]	×	×	♦ ▲ ■	♦ ▲ ■	×	|

PII in Plaintext in the Android File System (PII – Storage Location, Reference).

1.	Pak Identity [61]	Full Name, Email ID, Password, Mobile Number, Citizen ID, Location Coordinates – cd /data/data/pk.gov.nadra.pakid/databases/RKStorage, cd/data/data/pk.gov.nadra.pakid/databases/RKStorage-journal, Fig. 2, Appx. C.
2.	Pakistan Citizen Portal [62]	Full Name, Mobile Number, Email ID, Citizen ID, Profession, Date of Birth (DoB), Physical Address, Religion, Gender, Blood Group – cd /data/data/com.govpk.citizensportal/shared_prefs/userPref.xml, cd/data/user/0/com.govpk.citizensportal/shared_prefs/userPref.xml, Fig. 6, Appx. D.
3.	Qeemat Punjab [39]	Full Name, Guardian Name, Mobile Number, Email ID, Profession, Gender, Citizen ID – cd /data/data/com.pitb.qeematpunjab/shared_prefs/focial-session.xml, Fig. 14a, Fig. 14b, Appx. E.
4.	SIMOSA [68]	Mobile Number – cd /data/data/com.jazz. jazzworld/shared_prefs/jazzB2C.prefs.xml, Fig. 17, Appx. F. Call-SMS Records (Last 24 hrs) – cd /data/data/com.jazz. jazzworld/shared_ prefs/jazzB2C.prefs.xml, Fig. 16, Appx. F.
5.	My Zong [59]	Mobile Number, Full Name, Coarse Location – cd /data/data/com.zong.customercare/shared_pref/com.zong.customercare_preferences.xml, Fig. 19, Appx. G.
6.	My Telenor [58]	Mobile Number – cd /data/data/com.telenor.pakistan.mytelenor/shared_prefs/PrefName.xml, cd /data/data/com.telenor.pakistan.mytelenor/shared_prefs/com.telenor.pakistan.mytelenor.xml, Fig. 23 Fig. 24, Appx. H.
7.	UPTCL [71]	–

Selected PII Housed by Apps. (Keys: D –> Days, Hrs –> Hours, Req. –> Required.)

	App Title	Call History (30 D, 14 D, 7 D, 24 Hrs)	SMS History (30 D, 14 D, 7 D, 24 Hrs)	Tax Certificate	Location Coordinates
1.	Pak Identity [61]	×	×	×	Req. (Fig. 1a, Appx. C).
2.	Pakistan Citizen Portal [62]	×	×	×	Req. (Fig. 8, Appx. D).
3.	Qeemat Punjab [39]	×	×	×	Req. (Fig. 11, Appx. E).
4.	SIMOSA [68]	✓, ✓, ✓, ✓	✓, ✓, ✓, ✓	✓	Optional.
5.	My Zong [59]	×, ×, ✓, ✓	×, ×, ✓, ✓	✓	Optional.
6.	My Telenor [58]	×, ×, ✓, ✓	×, ×, ✓, ✓	✓	Optional.
7.	UPTCL [71]	×, ✓, ✓, ✓	×, ✓, ✓, ✓	✓	Optional.

file system, as shown in Table 4. This storage practice exposes user data to significant risks in case of device confiscation or theft, enabling attackers to exfiltrate personal credentials. The symbols, ♦, ▲, and ■ in Table 4 for “exposed PII” indicate that all three attacker types (i.e., state actors, private attackers, and hybrid actors) can exploit this attack vector prevalent in government apps. Moreover, all three apps cannot detect unauthorized logins from unknown devices or locations, leaving users vulnerable to security breaches.

All three government apps use TLS encryption, which is good, but this alone does not address the security and privacy needs of at-risk users in Pakistan. However, a corrupt state actor with a server private key can observe the traffic in plaintext and intercept and modify it. We successfully intercepted and modified the traffic for all three government apps. The exploit related to this vulnerability is to plant fake evidence.

8.1.1 ***Exploitation – Exposed PII.***

All three government apps transmit location data to their servers, creating a potential attack vector for state and hybrid actors. These actors, who may be able to confiscate an at-risk user’s device or access credentials from the app servers, can exploit this vulnerability through the following sequence: ❶ The at-risk user installs and uses the government apps on their phone. ❷ A state or hybrid actor confiscates the user’s device, or a private attacker steals the device. ❸ The attacker gains root access to the device and retrieves sensitive personal information (PII), such as the user’s full name, mobile number, and precise location coordinates. By exploiting the data stored on the device, attackers can track and monitor the user’s activities in real time. This sequence allows for both physical and digital compromises, enabling attackers to target at-risk individuals by accessing sensitive data on the device and monitoring their movements.

A related attack scenario involves the abuse of location data. ❶ The at-risk user uses the government app from home. ❷ The user uses the app from their workplace. ❸ At a later point, the user uses the app from a protest or rally. ❹ Each time the app is used, the location coordinates are transmitted to the app’s server. If attackers, such as state or hybrid actors, can retrieve credentials from the app server, they can map the entire geo-history of the at-risk user. That enables them to track the user’s movements across different locations—home, work, or even sensitive sites like protests—thereby enabling surveillance and potentially targeting the user based on their activity.

8.1.2 ***Exploitation – Missing Login Security Gap.***

All three government apps cannot detect login activity from unknown devices or locations, creating a significant vulnerability. The attack vector unfolds as follows: ❶ An at-risk user is using one of the government apps on their device. ❷ An attacker, such as a corrupt state actor with access to the server private key, observes the traffic in plaintext and captures the victim’s username and password when these credentials are sent to the app’s server (for example, the Pak Identity app transmits the username and password to the server shanakht.nadra.gov.pk, as shown in Fig. 1a and App. C). ❸ The attacker then uses these stolen credentials to log into the at-risk user’s account, intending to steal sensitive information or plant false evidence. ❹ Since the apps lack mechanisms to detect suspicious login activity, such as logins from unknown devices or unfamiliar locations, the user is never alerted to the breach. As a result, the attacker can continue to access the account without prompting the user to change their password or take any corrective action. This vulnerability allows attackers to exploit the lack of login activity monitoring and continue targeting users without detection.

8.1.3 ***Exploitation – Network Security Threats.***

Given recent developments in Pakistan, where local police have reportedly used geo-fencing data to track the whereabouts of protesters and activists at rallies [42], the potential misuse of this data has raised significant concerns. In particular, there is a growing fear that malicious actors could exploit geo-fencing data to plant false location coordinates as part of a personal vendetta, leading to the wrongful arrest of individuals at risk. The exploit could unfold as follows: ❶ An at-risk user uses government apps. ❷ A state actor—or a corrupt state actor—who has access to the server’s private key can view traffic in plaintext. ❸ The attacker then modifies the location coordinates in the intercepted request, replacing them with fabricated data. ❹ The altered request is sent to the server, where the false location coordinates are stored and potentially used as evidence for the arrest of an innocent individual. This type of exploit poses serious risks, as falsified location data could be presented as legitimate proof of an individual’s presence at a protest or other sensitive event, leading to legal or personal consequences for the at-risk users.

8.2 Telco Apps – SIMOSA, My Zong, My Telenor, UPTCL

All telco apps exhibit security gaps related to password and login protection, reflected in Table 4 with a ♦ ▲ ■ for missing password and login detection, indicating that all three attacker types can exploit this vulnerability. The four telco apps have implemented SSL pinning and use TLS encryption, so they are marked with a cross (×) in Table 4 for missing TLS vulnerabilities.

We partially bypassed SSL pinning on SIMOSA and UPTCL app, meaning some requests successfully reached the server while others triggered a “client handshake failed" message. As for manipulating PDF data in tax files, we have been unable to spoof this information. Because we could not eavesdrop on user credentials (such as mobile number of at-risk user, call or SMS history) and spoof information, we marked the traffic eavesdrop and modify section as inconclusive (|) for now for these apps. We bypassed SSL pinning for the My Zong and My Telenor apps and observed the user’s mobile number, call, and SMS history in-app traffic but could not spoof this information. So, we have used the notation ♦̆ ▲̆ ■̆ in Table 4 to indicate that eavesdropping of user credentials is possible with these two apps by all three types of attacker (state, private, and hybrid).

Table 4 shows three telco apps that lack root detection capabilities. All apps store call history, SMS records, and tax certificates (Fig. 15, App. F; Fig. 22, App. G; Fig. 25, App. H; Fig. 29, App. I) for specific periods. For example, the SIMOSA [68] app retains call history and SMS records for the last 30 days, 7 days, and 24 hours. Because it keeps data for the previous 30 days, retrieving call and SMS records from the past 14 days is possible. Similarly, the UPTCL app stores call and SMS history for the last 14 and 7 days, including records from the previous 24 hours.

Exploitation – Exposed PII + Missing Password + Network Security Threats. Due to the absence of a user-specified password and the missing feature of detecting unknown login activity, the following attack vector will work. ❶ A user device containing no photos, call, or SMS history is confiscated, stolen, or usurped by one of the attacker types in Table 2. ❷ An attacker obtains an at-risk user's mobile number via root access to the Android File System or Open Source Intelligence (OSINT) or eavesdropping (by compromised server private key). ❸ The corresponding app is (already) installed on the phone, or the attacker has installed it. ❹ The attacker enters the victim's mobile number on the confiscated, stolen, or usurped device, receives a One Time Password (OTP), and logs into the user account. ❺ Depending on the app, the attacker may receive another OTP to view call history SMS records and the information on the tax certificate. An exciting thing about this attack is that it would work even if the attacker had installed the app on the user's device.

9 RELATED WORK

This section discusses previous research examining apps for security and privacy risks.

9.0.1 Chat Apps. Espinoza et al. [76] reverse-engineered the LINE messaging app and identified a replay attack vulnerability due to weak encryption. In 2021, Lin [80] analyzed TikTok and Douyin, revealing dynamic source code loading and server-side censorship in Douyin. In 2023, Wang et al. [40] examined WeChat's tracking system, discovering significant user activity data being transmitted to the app's servers.

9.0.2 Healthcare Apps. In 2020, an analysis of the COVID-KAYA app revealed a vulnerability in its authentication logic, exposing the names of 30,000 healthcare providers [82]. Similarly, reverse engineering of the IATA Travel Pass app [81] revealed a critical flaw in its registration process that allowed attackers to impersonate users using only passport details without physical access to the passport itself.

9.0.3 Other Apps. Other significant reverse engineering efforts include studies that reveal personal data leakage in widely used Asian web browsers [78]. In 2021, Security Detectives [10] discovered that the Pakistani Bykea [48] app exposed 200 GB of user data on an unsecured Elasticsearch server. In 2023, researchers found a weak encryption system in Tencent's Sogou input method, allowing eavesdropping on real-time user input [44]. Kujath et al. [79] identified risks to user privacy in Latin American apps.

Although previous studies have provided valuable information on various global security and privacy risks, our analysis explicitly focuses on the leading Pakistani mobile apps. Using the tools and techniques of previous research, we address a gap in the literature on apps in Pakistan. This region has yet to be as extensively analyzed regarding security and privacy. Specifically, we explore unique risks and vulnerabilities prevalent in local apps, including those tied to government services and telcos. This targeted investigation builds on existing frameworks while offering new insights into Pakistani users' security challenges.

10 RECOMMENDATIONS

This section provides general recommendations for users, advocates, and app developers to help mitigate privacy risks. These recommendations should be customized according to an individual's specific risk profile, threat model, and objectives. For example, telco apps are often indispensable for tasks such as online bill payments, accessing tax certificates, and taking advantage of promotional offers, making them unavoidable for many users. Similarly, government apps facilitate updating citizen identity documents, reporting corruption, and obtaining information about agricultural product prices. Although no direct intervention can eliminate privacy risks associated with these apps, their necessity underscores the importance of conducting thorough privacy analyses on widely used apps (essential) for accessing government or telco services.

10.1 Recommendations for Users and Advocates

To protect privacy, we recommend that users minimize OS permissions and avoid using these apps in sensitive locations, as they may transmit location data.[3] Install government apps only when necessary and uninstall them immediately after use. Exercise caution with VPNs, as government apps transmit sensitive location data, and VPN use must be registered with the Pakistan Telecommunication Authority (PTA) [74]. VPNs can inadvertently expose real locations and traffic to ISPs. Since government and telco apps lack detection for logins from unfamiliar devices or locations, users should update passwords regularly and be cautious of unsolicited OTPs, which may signal account compromise. Enabling a remote data erasure feature is also advised.[4] Finally, we urge researchers, trainers, and advocates to address the gap between existing TLS protections and the specific privacy needs of at-risk users in Pakistan.

10.2 Recommendations for App Developers

The complex and rapidly evolving privacy and surveillance regulations in Pakistan [29], coupled with the lack of precise data protection guidelines, present significant challenges. To bridge this gap, we recommend app developers adopt globally recognized frameworks like the GDPR [52] and CCPA [49] to ensure robust privacy safeguards and compliance with international standards.

Developers should embed these principles throughout the app development lifecycle, including data minimization to collect only essential information, encrypting data at rest using NIST 800-111 guidelines [1], and implementing strong password protection and multi-factor authentication to prevent unauthorized access [75]. Proactively adopting these measures will enhance user trust and prepare apps for future regulatory changes, balancing innovation with privacy protection in a data-driven world.

11 CONCLUSION

In this paper, we analyzed a selection of leading Pakistani mobile apps to assess their security and privacy protections. Our findings revealed critical issues across three key categories: (i) excessive

[3] Government apps require location permissions to function, and telco apps need them to provide region-specific offers.

[4] With Android holding a 95% market share in Pakistan [57], most new phones include this capability.

collection and exposure of PII, (ii) gaps in password and login security, and (iii) flaws in network security. These vulnerabilities are particularly concerning given the heightened risks faced by journalists, civil rights defenders, and victims of domestic abuse in the region. They highlighted the persistent and widespread threats of surveillance and targeted malware attacks, which remain prevalent in the latest versions of major apps.

These mobile apps remain highly vulnerable due to their vast user bases, creating extensive attack surfaces. For example, a low-budget attacker—such as a domestic abuser—can quickly seize control of a victim's device, install the telco app (if not already installed), and access the victim's call and SMS history, thereby monitoring their communications and identifying their contacts. Similarly, state-sponsored attackers can target at-risk individuals like journalists or activists by confiscating their devices and extracting sensitive data (such as call and SMS records) via vulnerable telco apps (regardless of whether the app is installed on the device or not) without the user's knowledge—even if the user has taken steps to delete this information.

The findings of this analysis are especially crucial in light of the increasing threats to privacy and security in the region. The vulnerabilities we identified expose sensitive personal data to exploitation by a range of malicious actors, from domestic abusers to state agents. Conducting this analysis is not only timely but necessary, as it draws attention to the urgent need for stronger privacy protections in apps that serve tens of millions of users. Given the growing risks vulnerable populations face, app developers and policymakers must take immediate action to address these security flaws.

12 ACKNOWLEDGMENTS

This work was supported by Sana Habib's fellowship with the Open Technology Fund's Information Controls Fellowship Program and the National Science Foundation under Grant CNS-2141547. Sana gratefully acknowledges Pakistan's non-profit digital rights foundation for hosting her and the anonymous contributors whose insights were instrumental in the app selection process. We also sincerely thank the anonymous reviewers and Shepherd for their constructive feedback, which greatly enhanced the quality of this work.

REFERENCES

[1] 2007. *Special Publication 800-111 Guide to Storage Encryption Technologies for End User Devices.* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf

[2] 2012. *he Federal Investigation Agency. STABILIZING PAKISTAN THROUGH POLICE REFORM.* https://www.jstor.org/stable/pdf/resrep48528.24.pdf

[3] 2016. *This Crooked System. Police Abuse and Reform in Pakistan.* https://www.hrw.org/report/2016/09/27/crooked-system/police-abuse-and-reform-pakistan

[4] 2020. *COVID-19 Gov PK.* https://play.google.com/store/apps/details?id=com.govpk.covid19&hl=en_US&gl=US

[5] 2020. *Getting Away with Murder.* https://cpj.org/reports/2020/10/global-impunity-index-journalist-murders/

[6] 2020. *Netwalker ransomware hits Pakistan's largest private power utility.* https://www.databreaches.net/netwalker-ransomware-hits-pakistans-largest-private-power-utility/

[7] 2020. *Zindagi.* https://play.google.com/store/apps/details?id=com.psca.mnc.zindagi&hl=en_US&gl=US

[8] 2021. *Absar Alam.* https://en.wikipedia.org/wiki/Absar_Alam

[9] 2021. *BYKEA data breach: Pakistani ride-hailing app exposed 400m records.* https://www.hackread.com/bykea-data-breach-pakistani-ride-hailing-app/

[10] 2021. *BYKEA data breach: Pakistani ride-hailing app exposed 400m records.* https://www.hackread.com/bykea-data-breach-pakistani-ride-hailing-app/

[11] 2021. *Journalist and activist Muhammad Zada Agra fatally shot in Pakistan.* https://cpj.org/2021/11/journalist-and-activist-muhammad-zada-agra-fatally-shot-in-pakistan/

[12] 2021. *NADRA rejects biometric database hacking allegation, seeks explanation.* https://www.biometricupdate.com/202111/nadra-rejects-biometric-database-hacking-allegation-seeks-explanation

[13] 2021. *Overseas Pakistani's Complaint.* https://play.google.com/store/apps/details?id=pk.pitb.gov.opc&hl=en_US&gl=US

[14] 2021. *Pakistan Using Israeli Surveillance Tech, Despite No Diplomatic Ties, Report Claims.* https://themedialine.org/by-region/pakistan-using-israeli-surveillance-tech-despite-no-diplomatic-ties-report-claims/

[15] 2021. *Shahid Zehri. Metro 1 News | Killed in Hub, Pakistan | October 10, 2021.* https://cpj.org/data/people/shahid-zehri/

[16] 2021. *Unidentified men attack, bind, and gag Pakistani journalist Asad Ali Toor at his home in Islamabad.* https://cpj.org/2021/05/unidentified-men-attack-bind-and-gag-pakistani-journalist-asad-ali-toor-at-his-home-in-islamabad/

[17] 2022. *E-portal.* https://play.google.com/store/apps/details?id=com.nitb.noc&hl=en_US&gl=US

[18] 2022. *Foreign Minister's Portal.* https://play.google.com/store/apps/details?id=com.nitb.foreignministry.foreign_ministry_portal&hl=en_US&gl=US

[19] 2022. *KP Women Safety App.* https://play.google.com/store/apps/details?id=com.psca.ppic3.womensafetykp

[20] 2022. *Pehchaan Balochistan App.* https://play.google.com/store/apps/details?id=org.psca.pehchaanbalochistan&hl=en_SG&gl=US

[21] 2022. *Supreme Court of Pakistan.* https://play.google.com/store/apps/details?id=pk.gov.supremecourt&hl=en_US&gl=US

[22] 2023. *2023 Country Reports on Human Rights Practices: Pakistan.* https://www.state.gov/reports/2023-country-reports-on-human-rights-practices/pakistan/

[23] 2023. *2023 Country Reports on Human Rights Practices: Pakistan.* https://www.state.gov/reports/2023-country-reports-on-human-rights-practices/pakistan/

[24] 2023. *Apk Extractor.* https://play.google.com/store/apps/details?id=braveheart.apps.apkextract&hl=en_US&gl=US

[25] 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/

[26] 2023. *City Islamabad App.* https://play.google.com/store/apps/details?id=com.gov.pk.ictadministration&hl=en_US&gl=US

[27] 2023. *Corruption in Spotlight as Pakistan's Economy Spirals.* https://news.gallup.com/poll/505973/corruption-spotlight-pakistan-economy-spirals.aspx

[28] 2023. *Hackers put over 2 million Pakistanis' private data for sale after restaurant software breach.* https://www.databreaches.net/hackers-put-over-2-million-pakistanis-private-data-for-sale-after-restaurant-software-breach/

[29] 2023. *The legal landscape for privacy and surveillance in Pakistan.* https://www.ibanet.org/legal-landscape-for-privacy-surveillance-in-Pakistan

[30] 2023. *May 09 Riots.* https://en.wikipedia.org/wiki/May_9_riots

[31] 2023. *The Mobile Gender Gap Report.* https://www.gsma.com/r/wp-content/uploads/2023/07/The-Mobile-Gender-Gap-Report-2023.pdf

[32] 2023. *NADRA Data Leaks.* https://www.nation.com.pk/08-Jul-2023/nadra-data-leaks

[33] 2023. *Pakistan Corruption Rank.* https://tradingeconomics.com/pakistan/corruption-rank

[34] 2023. *Pass Track.* https://play.google.com/store/apps/details?id=com.passtrack.nitb.gov.pk&hl=en_US&gl=US

[35] 2023. *PTA CMS.* https://play.google.com/store/apps/details?id=pk.gov.pta.cms&hl=en_US&gl=US

[36] 2023. *Punjab Anti Dengue.* https://play.google.com/store/apps/details?id=dengue.tracking.system&hl=en_US&gl=US

[37] 2023. *Punjab Police-Women Safey App.* https://play.google.com/store/apps/details?id=com.psca.ppic3.womensafety&hl=en_US&gl=US

[38] 2023. *Qaumi Sehat Card.* https://play.google.com/store/apps/details?id=pk.gov.pitb.npsc&hl=en_US&gl=US

[39] 2023. *Qeemat Punjab.* https://play.google.com/store/apps/details?id=com.pitb.qeematpunjab&hl=en_US&gl=US

[40] 2023. *Should We Chat? Privacy in the WeChat Ecosystem.* https://citizenlab.ca/2023/06/privacy-in-the-wechat-ecosystem-full-report/

[41] 2023. *'They Can Kill Me At Any Time': Pakistani Journalist Recalls Kidnapping And Alleged Torture By Militants.* https://www.rferl.org/a/pakistan-journalist-attacked-abducted-press-freedom/32393605.html

[42] 2023. *The use of Geofencing techinques and Call Data Records (CDR) as means of investigation in Pakistan.* https://joshandmakinternational.com/geofencing-and-the-law-in-pakistan/#:~:text=These%20techniques%20use%20biometrics%20to,the%20absence%20of%20proper%20constitutional

[43] 2023. *What Are SSL Stripping Attacks?* https://venafi.com/blog/what-are-ssl-stripping-attacks/

[44] 2023. *"Please do not make it public" Vulnerabilities in Sogou Keyboard encryption expose keypresses to network eavesdropping.* https://citizenlab.ca/2023/08/vulnerabilities-in-sogou-keyboard-encryption/

[45] 2024. *Android Debug Bridge (adb).* https://developer.android.com/tools/adb
[46] 2024. *Android Version Market Share Pakistan Dec 2023 - Dec 2024.* https://gs.statcounter.com/android-version-market-share/all/pakistan
[47] 2024. *APKPure.* https://apkpure.net/
[48] 2024. *Bykea: Rides & Delivery App.* https://play.google.com/store/apps/details?id=com.bykea.pk&hl=en_US&gl=US
[49] 2024. *California Consumer Privacy Act (CCPA).* https://oag.ca.gov/privacy/ccpa
[50] 2024. *E-Services Sindh.* https://play.google.com/store/apps/details?id=pk.pitb.gov.eServicesSindh&hl=en_US&gl=US
[51] 2024. *ePay Punjab.* https://play.google.com/store/apps/details?id=com.pitb.ePayGateway&hl=en_US&gl=US
[52] 2024. *General Data Protection Regulation.* https://gdpr-info.eu/
[53] 2024. *Google Play Store.* https://play.google.com/store/games?hl=en_US
[54] 2024. *Inside the Punitive State: Governance Through Punishment in Pakistan.* https://carnegieendowment.org/research/2024/06/pakistan-punitive-state-terrorism-police?lang=en
[55] 2024. *Jazz strengthens its market share to 37pc with 71m subscribers.* https://www.brecorder.com/news/40286306
[56] 2024. *List of telecommunication companies in Pakistan.* https://en.wikipedia.org/wiki/List_of_telecommunication_companies_in_Pakistan
[57] 2024. *Mobile Operating System Market Share Pakistan.* https://gs.statcounter.com/os-market-share/mobile/pakistan
[58] 2024. *My Telenor.* https://play.google.com/store/apps/details?id=com.telenor.pakistan.mytelenor&hl=en_US
[59] 2024. *My Zong.* https://play.google.com/store/apps/details?id=com.zong.customercare&hl=en_US
[60] 2024. *On eve of elections in Pakistan, RSF calls for clear safeguards for right to information.* https://rsf.org/en/eve-elections-pakistan-rsf-calls-clear-safeguards-right-information
[61] 2024. *Pak Identity.* https://play.google.com/store/apps/details?id=pk.gov.nadra.pakid&hl=en_US&gl=US
[62] 2024. *Pakistan Citizen Portal.* https://play.google.com/store/apps/details?id=com.govpk.citizensportal&hl=en_US&gl=US
[63] 2024. *Pakistan PM Sharif removes 25 senior tax officers for corruption: Report.* https://www.business-standard.com/world-news/pakistan-pm-sharif-removes-25-senior-tax-officers-for-corruption-report-124042700694_1.html
[64] 2024. *PCAPdroid - network monitor.* https://play.google.com/store/apps/details?id=com.emanuelef.remote_capture&hl=en_US
[65] 2024. *Prominent Baluch Activist Stopped From Leaving Pakistan For U.S. Event.* https://www.rferl.org/a/pakistan-baloch-baluch-rights-travel-ban/33151431.html
[66] 2024. *Punjab Police Pakistan.* https://play.google.com/store/apps/details?id=pk.pitb.gov.ppcma&hl=en_US&gl=US
[67] 2024. *RSF calls for urgent measures by Pakistan's new government to rebuild press freedom.* https://rsf.org/en/rsf-calls-urgent-measures-pakistan-s-new-government-rebuild-press-freedom
[68] 2024. *SIMOSA - Jazz World.* https://play.google.com/store/apps/details?id=com.jazz.jazzworld&hl=en_US
[69] 2024. *Telecom Companies in Pakistan: A Panoptic Surveillance System.* https://gsdn.live/telecom-companies-in-pakistan-a-panoptic-surveillance-system/
[70] 2024. *Unleash the power of Frida.* https://codeshare.frida.re/
[71] 2024. *UPTCL– App Up Your Life!* https://play.google.com/store/apps/details?id=com.ufoneselfcare&hl=en_US
[72] 2024. *Wireshark.* https://www.wireshark.org/
[73] 2024. *Zong (mobile network).* https://en.wikipedia.org/wiki/Zong_(mobile_network)
[74] 2025. *Pakistan Requires People to Register Their VPN Use.* https://www.cyberghostvpn.com/privacyhub/pakistan-register-vpn/
[75] Periwinkle Doerfler, Kurt Thomas, Maija Marincenko, Juri Ranieri, Yu Jiang, Angelika Moscicki, and Damon McCoy. 2019. Evaluating login challenges as adefense against account takeover. In *The World Wide Web Conference.* 372–382.
[76] Antonio M Espinoza, William J Tolley, Jedidiah R Crandall, Masashi Crete-Nishihata, and Andrew Hilts. 2017. Alice and bob, who the {FOCI} are they?: Analysis of end-to-end encryption in the {LINE} messaging application. In *7th USENIX Workshop on Free and Open Communications on the Internet (FOCI 17).*
[77] Hamida Khatri. 2020. Domestic Violence in Pakistan from 1990–2020: A Mixed Method Approach. (2020).
[78] Jeffrey Knockel, Adam Senft, and Ronald Deibert. 2016. Privacy and Security Issues in {BAT} Web Browsers. In *6th USENIX Workshop on Free and Open Communications on the Internet (FOCI 16).*
[79] Beau Kujath, Jeffrey Knockel, Paul Aguilar, Diego Morabito, Masashi Crete-Nishihata, and Jedidiah R Crandall. 2024. Analyzing Prominent Mobile Apps in Latin America. *Free and Open Communications on the Internet* (2024).
[80] Pellaeon Lin. 2021. *TikTok vs Douyin A Security and Privacy Analysis.* Citizen Lab Research Report Number 132. University of Toronto, Canada.
[81] Pellaeon Lin. 2022. *Privacy and Security Analysis of the IATA Travel Pass Android App.* Citizen Lab Research Report Number 154. University of Toronto, Canada.
[82] Jeffrey Knockel Adam Senft Irene Poetranto Stephanie Tran Pellaeon, Lin and Deibert Ron. 2020. *Unmasked: COVID-KAYA and the Exposure of Healthcare Worker Data in the Philippines.* Citizen Lab Research Repor 132. Massachusetts Institute of Technology, University of Toronto, Canada.

A PAKISTANI APPS SELECTION CRITERIA

Although numerous Pakistani apps serve various citizen services, evaluating each can be overwhelming. This study aims to comprehensively analyze state-sponsored and commercial Pakistani apps, providing insight into the ecosystem without requiring exhaustive evaluations of every app. To achieve this, we selected a focused subset of both state-owned and commercial apps that significantly impact individuals' security and privacy. The selection process involved compiling a list of apps based on factors such as popularity, necessity, and data collection practices and then refining this list using explicit review criteria for a targeted examination. Here is how we curated our candidate set of apps.

A.1 Popularity

Popularity was a key metric for selecting local apps. We measured this through the number of downloads. For example, the state-sponsored Pak Identity app [61], with over 1M downloads, is more popular than the City Islamabad app [26], which has around 500K downloads.

A.2 Necessity

The necessity of use was another crucial factor. Apps widely used by the public, such as the Pak Identity app [61] for requesting or updating identity documents, were prioritized. Similarly, telco apps like SIMOSA [68], My Zong [59], My Telenor [58], and UPTCL [71] were considered essential for tasks like downloading tax certificates, eliminating the need for in-person visits.

A.3 Timeliness

Timeliness significantly influenced the selection process. For example, as the pandemic is under control, people use COVID-related apps less frequently. Similarly, the lack of updates on apps since before 2020 indicated that they were no longer in active use.

A.4 Personal Data Collection

User registration requirements were a pivotal metric for app selection. That is because access to user credentials, particularly sensitive data like location coordinates, increases the risk of surveillance or exploitation by state or non-state actors if not adequately protected.

A.5 Local Situation

The local context in Pakistan was a key factor in our selection process. For example, recent cases where local police used geofencing data to arrest protestors highlighted the importance of state-sponsored apps collecting location data [30]. Similarly, instances where local authorities coerced telcos to share personal data underscored the significance of telco apps in this ecosystem [69].

Table 5 provides an overview of the selected Pakistani apps and their corresponding categories.

Table 5: Pakistani Apps Repository.

	App Category	App Title
1.	Accountability	(i) Pakistan Citizen Portal [62], (ii) Supreme Court of Pakistan [21], (iii) Qeemat Punjab [39], (iv) Overseas Pakistani's Complaint [13], (v) Foreign Minister's Portal [18].
2.	Database & Registration	(i) Pak Identity [61], (ii) ePay Punjab [51], (iii) City Islamabad App [26], (iv) E-portal [17], (v) E-Services Sindh [50], (vii) PTA CMS [35].
3.	Health Care	(i) Pass Track [34], (ii) COVID-19 Gov PK [4], (iii) Qaumi Sehat Card [38], (iv) Punjab Anti Dengue [36],
4.	Safety	(i) Punjab Police Pakistan [66], (ii) Pehchaan Balochistan App [20], (iii) Punjab Police-Women Safety App [37], (iv) KP Women Safety App [19], (v) Zindagi [7].
5.	Telco	(i) SIMOSA [68], (ii) My Zong [59], (iii) My Telenor [58], (iv) UPTCL [71].

Reverse engineering and testing Android apps require a substantial time investment. Each app requires installation, account creation, verification, and thorough operational testing. Our methodology includes manual review of privacy policies, analysis of PII stored in the Android File System, analysis of source codes for suspicious packages and hard-coded secrets, and capture of traffic to assess transport layer security. Given the labor-intensive nature of these tasks, evaluating all 25 apps (in Table 5) was impractical. To address this, we established a prioritization framework based on the features outlined above (A.1, A.2, A.3, A.4, and A.5), enabling us to create a stratified sample that represents the broader ecosystem of Pakistani apps.

Our final list includes seven apps that provide a snapshot of the ecosystem. These apps were reverse-engineered and evaluated. They fall into two main categories: state-sponsored apps, typically developed by government-affiliated entities or outsourced to third-party companies, and commercial apps created by private companies. Similar organizations often develop these apps, and they are likely to share common security and privacy vulnerabilities. Therefore, the seven apps listed in Table 1 offer valuable insights into the broader ecosystem.

B THREAT CLASSIFICATION DETAILS

In Pakistan, where state actors often seize devices and non-state actors can steal them, the security of personal information is critical. The risks associated with excessive PII collection, weak password security, and compromised network traffic (via server private key compromise) are heightened by the local context, where surveillance and data exploitation are frequent. These threats can lead to significant breaches of user privacy, especially when sensitive information is exposed or intercepted by malicious actors.

B.1 Unnecessary Disclosure

The first threat we evaluated for each app is the excessive PII collection and the associated data leakage risk. That occurs when an app collects more data than necessary for its core functionality. Data leakage happens when sensitive information—such as a user's full name, phone number, or email address—is transmitted to a server without clear disclosure in the app's privacy policy, user agreement, or app store description.

The risks are further compounded when PII is stored in plaintext within the root directory of the Android file system, with no mention of this in the privacy policy or user agreement. Many users, even those with root access, are unaware of how their data is stored beyond the SD card, which leaves them vulnerable. This lack of transparency increases the likelihood that physical attackers—such as law enforcement or criminal actors, like those involved in drug trafficking—can access sensitive information if they confiscate or steal the device. In Pakistan, where state actors frequently seize devices and domestic abusers may take control of the device with or without the user's consent and knowledge, these security gaps expose users to significant risks. Communications, including call and SMS histories, can be monitored and exploited, further jeopardizing user privacy and safety.

B.2 Login Weaknesses

Given that state actors can confiscate mobile devices and non-state actors can steal them, the second threat we examined in each app was the absence of a user password and the lack of a feature to detect unknown login activity. We evaluated how easily an attacker could log into an at-risk user's account and access sensitive information, such as location coordinates, physical address, call history, and SMS records. In the absence of a mechanism to detect unknown login activity, attackers, such as ISPs or domestic abusers, can access the victim's account and monitor their activities without alerting the user. This lack of notification significantly increases the risk of unauthorized access and misuse of personal information.

B.3 Network Security Threats

The third threat involves network security risks, which allow local or in-path attackers to eavesdrop on or manipulate network traffic, potentially compromising the app's functionality. This risk amplifies when the app uses unencrypted protocols like HTTP to interact with the application servers or third-party services. The threat becomes even more significant if the attacker possesses a server private key, enabling them to intercept and modify data in real time (often in formats like JSON or PDF). This vulnerability could allow an attacker to spoof critical data, such as location coordinates, thereby fabricating false evidence of the user's presence at a sensitive location at a specific time.

C PAK IDENTITY APP

This subsection explains the snapshots of the test results for the Pak Identity app. The user credentials of interest are marked using an orange rectangle in all the figures. Some sensitive user credentials, such as citizen number, mobile number, and password, have been redacted in the statistics because they are in plaintext.

Fig. 1a represents the client's authentication request to the server (with redacted *password*, which is in plaintext). Fig. 1b shows the server's response to the client's request (with redacted *citizen number* and *mobile number*). Fig. 2 shows a collection of user credentials in plaintext. Fig. 1c shows planting fake evidence via JSON spoofing, whereby fake location coordinates of latitude: 0 and longitude: 0 have replaced the original location coordinates of latitude: 33.41.. and longitude: -111.90.. in Fig. 1a.

Fig. 3 shows PDF spoofing, whereby the original instructions for capturing fingerprints (Fig. 3a) have been replaced by spoofed instructions (Fig. 3b). The spoofed or fake PDF file gets stored in the Android file system. Thus, PDF spoofing is an easily exploitable attack vector for planting (fake) evidence in an at-risk user's device.

D PAKISTAN CITIZEN PORTAL APP

This subsection explains the snapshots of the test results for the Pakistan Citizen Portal app. Fig. 4 shows the device credentials sent to the *api.pmdu.gov.pk* server at login. Fig. 5a and Fig. 5b show sensitive user credentials collected with user registration in the response message. We have redacted user credentials because they are in plaintext. These sensitive user credentials are stored in plaintext in the Android file system (shown in Fig. 6a and Fig. 6b). Fig. 8a and Fig. 8b show the PII (including location coordinates) that are collected when an at-risk user submits a suggestion.

Fig. 9 shows JSON data spoofing, whereby fake location coordinates of latitude:0 and longitude:0 (Fig. 9b, Fig. 9c) have replaced the original location coordinates of latitude: 33.41.. and longitude: -111.90... (in Fig. 9a). Fig. 7 shows the Pakistan Citizen Portal app's original and spoofed terms and conditions.

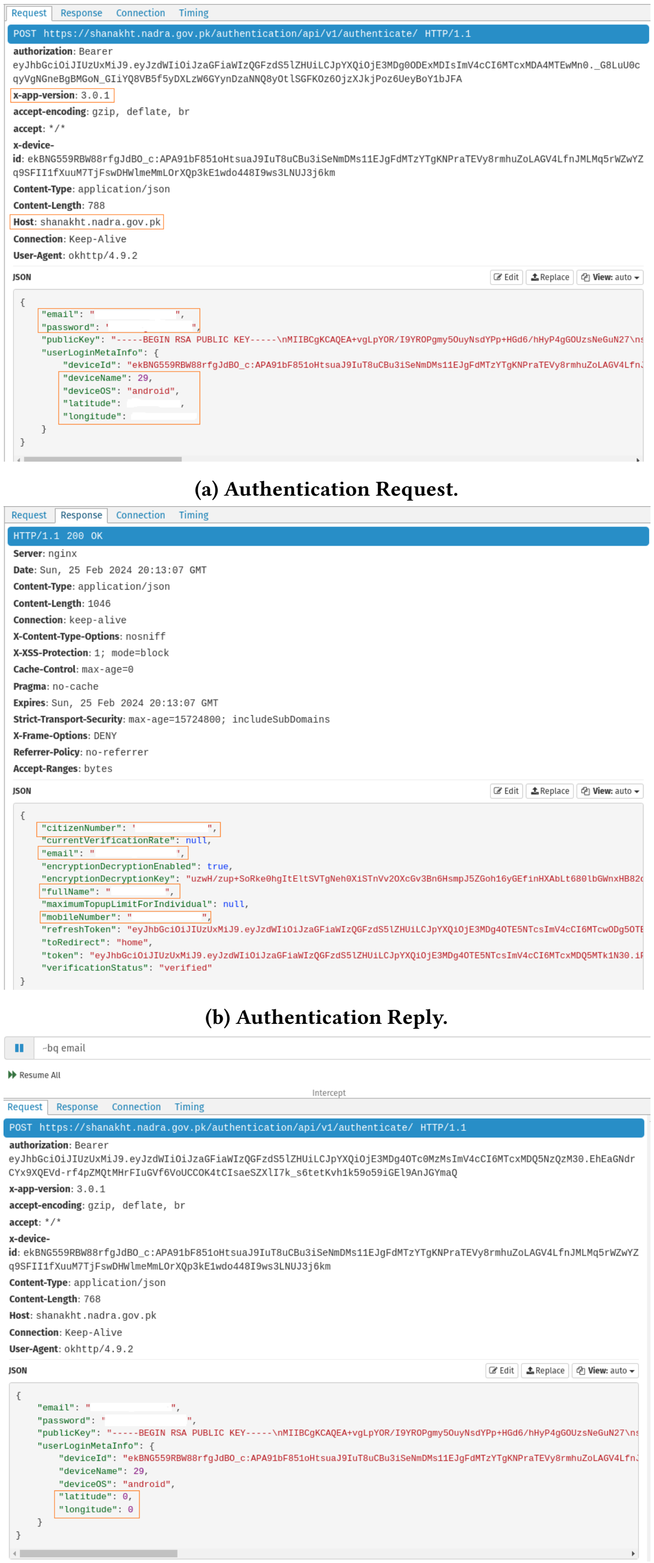
E QEEMAT PUNJAB APP

This subsection explains the snapshots of the results for the Qeemat Punjab app [39]. Fig. 10 shows the PII collected by the app (including gender, guardian name, physical address, and national identity number). Fig. 11 shows that the app collected precise location coordinates when submitting a suggestion (location coordinates are transmitted when submitting a complaint).

The Qeemat Punjab app is vulnerable to JSON data spoofing. Fig. 12a shows the original location coordinates when submitting a suggestion, and Fig. 12b shows the fake or planted location coordinates when submitting a suggestion. Fig. 14a and Fig. 14b show storage of user credentials in plaintext in the Android file system. Fig. 13a and Fig. 13b show poultry products' original and spoofed prices.

F SIMOSA APP

Figures 17, 18, and 16 show that the user's mobile number, device details, and call-SMS history are stored in plaintext in the root directory of the Android File System for the SIMOSA app [68]. Fig. 15 shows the tax certificate generated by the app. The tax certificate contains a username, physical address, CNIC number, and mobile number.



```
POST https://shanakht.nadra.gov.pk/authentication/api/v1/authenticate/ HTTP/1.1
authorization: Bearer
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJzaGFiaWIzQGFzdS5lZHUiLCJpYXQiOjE3MDg0ODExMDIsImV4cCI6MTcxMDA4MTEwMn0._G8LuU0c
qyVgNGneBgBMGoN_GIiYQ8VB5f5yDXLzW6GYynDzaNNQ8yOtlSGFKOz6OjzXJkjPoz6UeyBoY1bJFA
x-app-version: 3.0.1
accept-encoding: gzip, deflate, br
accept: */*
x-device-
id: ekBNG559RBW88rfgJdBO_c:APA91bF851oHtsuaJ9IuT8uCBu3iSeNmDMs11EJgFdMTzYTgKNPraTEVy8rmhuZoLAGV4LfnJMLMq5rWZwYZ
q9SFII1fXuuM7TjFswDHWlmeMmLOrXQp3kE1wdo448I9ws3LNUJ3j6km
Content-Type: application/json
Content-Length: 788
Host: shanakht.nadra.gov.pk
Connection: Keep-Alive
User-Agent: okhttp/4.9.2
JSON
{
    "email": "[redacted]",
    "password": '[redacted]",
    "publicKey": "-----BEGIN RSA PUBLIC KEY-----\nMIIBCgKCAQEA+vgLpYOR/I9YROPgmy5OuyNsdYPp+HGd6/hHyP4gGOUzsNeGuN27\ns
    "userLoginMetaInfo": {
        "deviceId": "ekBNG559RBW88rfgJdBO_c:APA91bF851oHtsuaJ9IuT8uCBu3iSeNmDMs11EJgFdMTzYTgKNPraTEVy8rmhuZoLAGV4LfnJ
        "deviceName": 29,
        "deviceOS": "android",
        "latitude": [redacted],
        "longitude": [redacted]
    }
}
```

(a) Authentication Request.

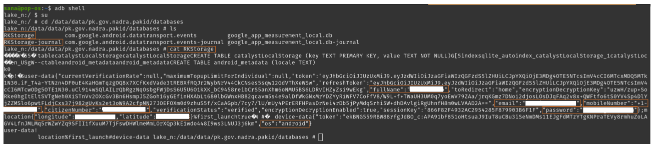
```
HTTP/1.1 200 OK
Server: nginx
Date: Sun, 25 Feb 2024 20:13:07 GMT
Content-Type: application/json
Content-Length: 1046
Connection: keep-alive
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: max-age=0
Pragma: no-cache
Expires: Sun, 25 Feb 2024 20:13:07 GMT
Strict-Transport-Security: max-age=15724800; includeSubDomains
X-Frame-Options: DENY
Referrer-Policy: no-referrer
Accept-Ranges: bytes
JSON
{
    "citizenNumber": '[redacted]",
    "currentVerificationRate": null,
    "email": "[redacted]',
    "encryptionDecryptionEnabled": true,
    "encryptionDecryptionKey": "uzwH/zup+SoRke0hgItEltSVTgNeh0XiSTnVv2OXcGv3Bn6HsmpJ5ZGoh16yGEfinHXAbLt680lbGWnxHB82c
    "fullName": "[redacted]",
    "maximumTopupLimitForIndividual": null,
    "mobileNumber": "[redacted]",
    "refreshToken": "eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJzaGFiaWIzQGFzdS5lZHUiLCJpYXQiOjE3MDg4OTE5NTcsImV4cCI6MTcwODg5OTE
    "toRedirect": "home",
    "token": "eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJzaGFiaWIzQGFzdS5lZHUiLCJpYXQiOjE3MDg4OTE5NTcsImV4cCI6MTcxMDQ5MTk1N30.iP
    "verificationStatus": "verified"
}
```

(b) Authentication Reply.

```
POST https://shanakht.nadra.gov.pk/authentication/api/v1/authenticate/ HTTP/1.1
authorization: Bearer
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJzaGFiaWIzQGFzdS5lZHUiLCJpYXQiOjE3MDg4OTc0MzMsImV4cCI6MTcxMDQ5NzQzM30.EhEaGNdr
CYx9XQEVd-rf4pZMQtMHrFIuGVf6VoUCCOK4tCIsaeSZXlI7k_s6tetKvh1k59o59iGEl9AnJGYmaQ
x-app-version: 3.0.1
accept-encoding: gzip, deflate, br
accept: */*
x-device-
id: ekBNG559RBW88rfgJdBO_c:APA91bF851oHtsuaJ9IuT8uCBu3iSeNmDMs11EJgFdMTzYTgKNPraTEVy8rmhuZoLAGV4LfnJMLMq5rWZwYZ
q9SFII1fXuuM7TjFswDHWlmeMmLOrXQp3kE1wdo448I9ws3LNUJ3j6km
Content-Type: application/json
Content-Length: 768
Host: shanakht.nadra.gov.pk
Connection: Keep-Alive
User-Agent: okhttp/4.9.2
JSON
{
    "email": "[redacted]",
    "password": "[redacted]",
    "publicKey": "-----BEGIN RSA PUBLIC KEY-----\nMIIBCgKCAQEA+vgLpYOR/I9YROPgmy5OuyNsdYPp+HGd6/hHyP4gGOUzsNeGuN27\ns
    "userLoginMetaInfo": {
        "deviceId": "ekBNG559RBW88rfgJdBO_c:APA91bF851oHtsuaJ9IuT8uCBu3iSeNmDMs11EJgFdMTzYTgKNPraTEVy8rmhuZoLAGV4LfnJ
        "deviceName": 29,
        "deviceOS": "android",
        "latitude": 0,
        "longitude": 0
    }
}
```

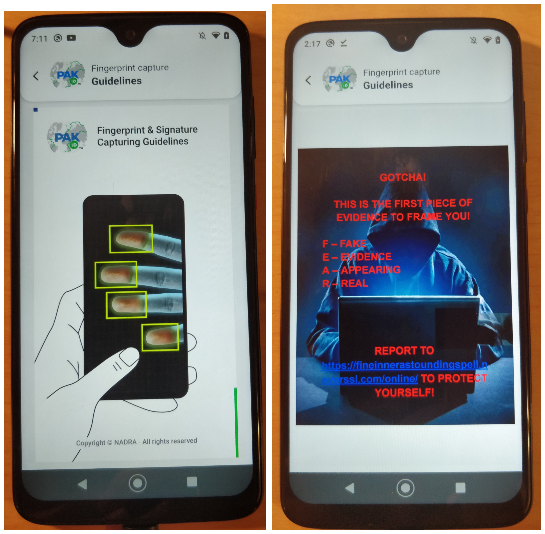
(c) Intercepted Authentication Request.

Figure 1: PII Collection and JSON Data Spoofing in the Pak Identity App [61].



```
sana@pop-os:~$ adb shell
lake_n:/ $ su
lake_n:/ # cd /data/data/pk.gov.nadra.pakid/databases
lake_n:/data/data/pk.gov.nadra.pakid/databases # ls
RKStorage         com.google.android.datatransport.events         google_app_measurement_local.db
RKStorage-journal com.google.android.datatransport.events-journal google_app_measurement_local.db-journal
lake_n:/data/data/pk.gov.nadra.pakid/databases # cat RKStorage
����w55�tablecatalystLocalStoragecatalystLocalStorageCREATE TABLE catalystLocalStorage (key TEXT PRIMARY KEY, value TEXT NOT NULL)G[5indexsqlite_autoindex_catalystLocalStorage_1catalystLoc
��en_USgW--ctableandroid_metadataandroid_metadataCREATE TABLE android_metadata (locale TEXT)
k0
k�p!�5user-data{"currentVerificationRate":null,"maximumTopupLimitForIndividual":null,"token":"eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJzaGFiaWIzQGFzdS5lZHUiLCJpYXQiOjE3MDg4OTE5NTcsImV4cCI6MTcxMDQ5MTk
1N30.iF_T4a-YtNzn4DF0uE4KaHGmTqzgOQ8x7XCfKxdVade3tREBXfRQJr2WybNrV44CkCNses5sqw12GdVThXeWSw","refreshToken":"eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJzaGFiaWIzQGFzdS5lZHUiLCJpYXQiOjE3MDg4OTE5NTcsImV4
cCI6MTcwODg5OTE1N30.uCl914wSQlAILrQbRgzNqOsbgFWjDsS6U5U6O1kXK_bC9458reibCrS5anXhm6oNMU5BS6LDRvIHZyZsi9wEkg","fullName":"[redacted]","toRedirect":"home","encryptionDecryptionKey":"uzwH/zup+So
Rke0hgItEltSVTgNeh0XiSTnVv2OXcGv3Bn6HsmpJ5ZGoh16yGEfinHXAbLt680lbGWnxHB82qcavm5s4e9alDfWkGNxMrYDZYyRiWFV7CoFfV8/W9L+f+TWaUH3UM0q7yoEwV79ZAa/jrqKGmz7DNoi2djosLOsDJqFAq2v8x+QWFtfo6tS0YV4Sp4DlY
jZZMSlo6pwtFLdjCxs37j982gUvKs2et3oW9A2cfpMN27JOEFOXm0d9zhuS5f/xCaAGpb/7cy7/lU/mUy4PErERFHPasDrNei4rDb5jPyMdqSrhi5W+dhDAvlgiRgUhnfH8m0wLVAAD2A==","email":"[redacted]","mobileNumber":"+1-
[redacted]","citizenNumber":"[redacted]","verificationStatus":"verified","encryptionDecryptionEnabled":true,"sessionKey":"866F82F4932AC2954285F879903B6F1F","password":"[redacted]"};m
location{"longitude":[redacted],"latitude":[redacted]}%first_launchtrue�M #� device-data{"token":"ekBNG559RBW88rfgJdBO_c:APA91bF851oHtsuaJ9IuT8uCBu3iSeNmDMs11EJgFdMTzYTgKNPraTEVy8rmhuZoLA
GV4LfnJMLMq5rWZwYZq9SFII1fXuuM7TjFswDHWlmeMmLOrXQp3kE1wdo448I9ws3LNUJ3j6km","os":"android"}
user-data!
        location%first_launch#device-data lake_n:/data/data/pk.gov.nadra.pakid/databases # 
```

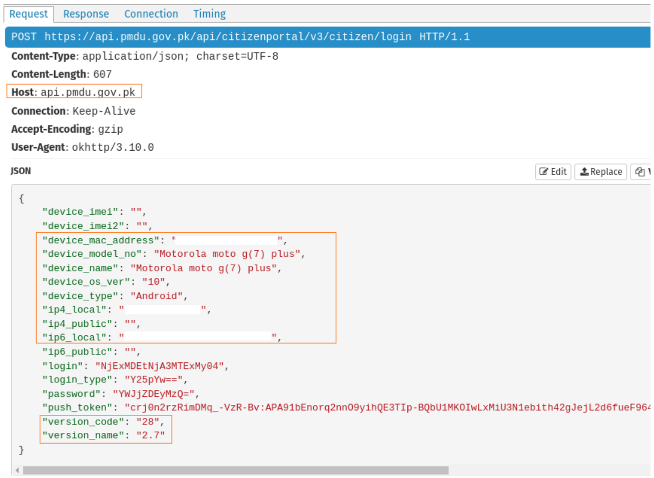
Figure 2: PII in Android File System for Pak Identity App [61].


7:11
Fingerprint capture
Guidelines
Fingerprint & Signature
Capturing Guidelines
Copyright © NADRA - All rights reserved
2:17
Fingerprint capture
Guidelines
GOTCHA!
THIS IS THE FIRST PIECE OF EVIDENCE TO FRAME YOU!
F – FAKE
E – EVIDENCE
A – APPEARING
R – REAL
REPORT TO https://fineinnerastoundingspell.neverssl.com/online/ TO PROTECT YOURSELF!

(a) Original.

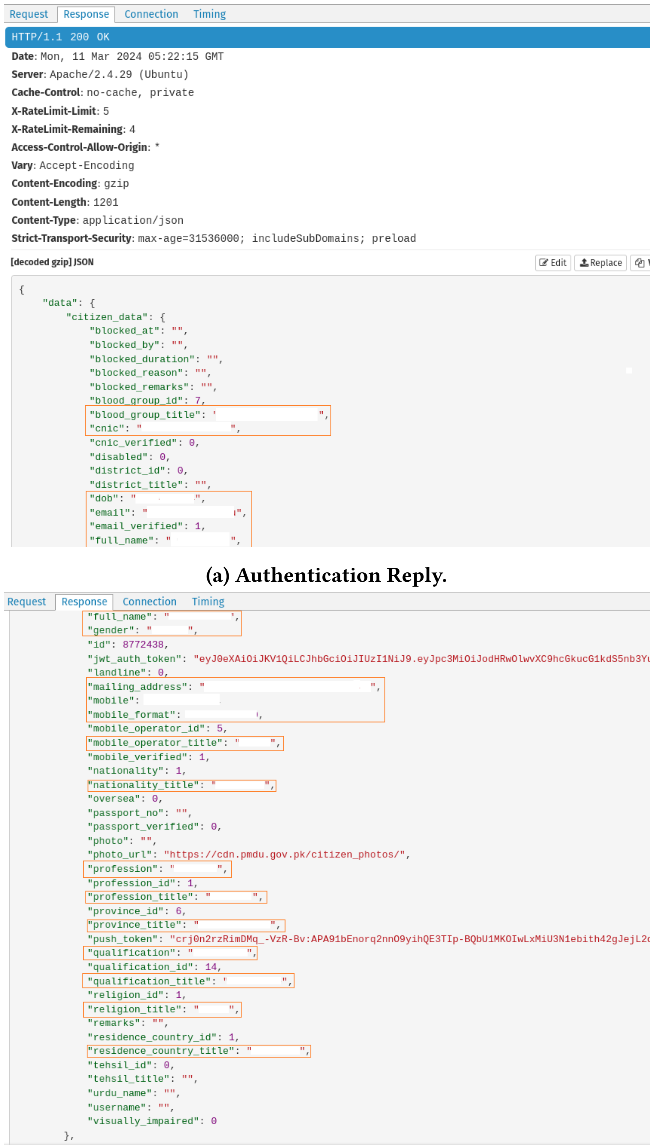
(b) Spoofed.

Figure 3: Original and Spoofed Fingerprint Capture Guidelines in the Pak Identity App [61].



```
POST https://api.pmdu.gov.pk/api/citizenportal/v3/citizen/login HTTP/1.1
Content-Type: application/json; charset=UTF-8
Content-Length: 607
Host: api.pmdu.gov.pk
Connection: Keep-Alive
Accept-Encoding: gzip
User-Agent: okhttp/3.10.0
JSON
{
    "device_imei": "",
    "device_imei2": "",
    "device_mac_address": "[redacted]",
    "device_model_no": "Motorola moto g(7) plus",
    "device_name": "Motorola moto g(7) plus",
    "device_os_ver": "10",
    "device_type": "Android",
    "ip4_local": "[redacted]",
    "ip4_public": "",
    "ip6_local": "[redacted]",
    "ip6_public": "",
    "login": "NjExMDEtNjA3MTExMy04",
    "login_type": "Y25pYw==",
    "password": "YWJjZDEyMzQ=",
    "push_token": "crj0n2rzRimDMq_-VzR-Bv:APA91bEnorq2nnO9yihQE3TIp-BQbU1MKOIwLxMiU3N1ebith42gJejL2d6fueF964
    "version_code": "28",
    "version_name": "2.7"
}
```

Figure 4: Authentication Request for Pakistan Citizen Portal App [62].



```
HTTP/1.1 200 OK
Date: Mon, 11 Mar 2024 05:22:15 GMT
Server: Apache/2.4.29 (Ubuntu)
Cache-Control: no-cache, private
X-RateLimit-Limit: 5
X-RateLimit-Remaining: 4
Access-Control-Allow-Origin: *
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 1201
Content-Type: application/json
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
[decoded gzip] JSON
{
    "data": {
        "citizen_data": {
            "blocked_at": "",
            "blocked_by": "",
            "blocked_duration": "",
            "blocked_reason": "",
            "blocked_remarks": "",
            "blood_group_id": 7,
            "blood_group_title": '[redacted]",
            "cnic": "[redacted]",
            "cnic_verified": 0,
            "disabled": 0,
            "district_id": 0,
            "district_title": "",
            "dob": "[redacted]",
            "email": "[redacted]",
            "email_verified": 1,
            "full_name": "[redacted]",
```

(a) Authentication Reply.

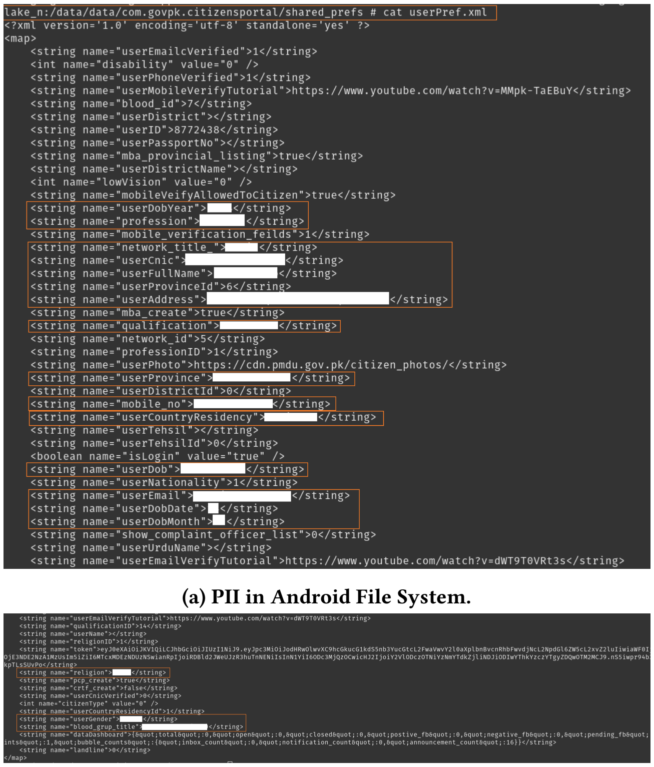
```
            "full_name": "[redacted]',
            "gender": "[redacted]",
            "id": 8772438,
            "jwt_auth_token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJodHRwOlwvXC9hcGkucG1kdS5nb3Yu
            "landline": 0,
            "mailing_address": "[redacted]",
            "mobile": [redacted]
            "mobile_format": [redacted],
            "mobile_operator_id": 5,
            "mobile_operator_title": "[redacted]",
            "mobile_verified": 1,
            "nationality": 1,
            "nationality_title": "[redacted]",
            "oversea": 0,
            "passport_no": "",
            "passport_verified": 0,
            "photo": "",
            "photo_url": "https://cdn.pmdu.gov.pk/citizen_photos/",
            "profession": "[redacted]",
            "profession_id": 1,
            "profession_title": "[redacted]",
            "province_id": 6,
            "province_title": "[redacted]",
            "push_token": "crj0n2rzRimDMq_-VzR-Bv:APA91bEnorq2nnO9yihQE3TIp-BQbU1MKOIwLxMiU3N1ebith42gJejL2c
            "qualification": "[redacted]",
            "qualification_id": 14,
            "qualification_title": '[redacted]",
            "religion_id": 1,
            "religion_title": "[redacted]",
            "remarks": "",
            "residence_country_id": 1,
            "residence_country_title": "[redacted]",
            "tehsil_id": 0,
            "tehsil_title": "",
            "urdu_name": "",
            "username": "",
            "visually_impaired": 0
        },
```

(b) Authentication Reply (continued..).

Figure 5: Authentication Reply for the Pakistan Citizen Portal App [62].

G MY ZONG APP

Figure 19 reveals that the My Zong app [59] stores sensitive user information, including the username, mobile number, and coarse location coordinates, in plaintext within the root directory of the Android File System. Furthermore, Figure 22 displays a tax certificate generated by the app, which exposes additional personal data such as the user's CNIC (Computerized National Identity Card) and mobile number. Figure 21 demonstrates that the app transmits the mobile number of an at-risk user to its server at myyzongapp-nlbt.zong.com.pk as part of a request to retrieve call history. Finally, Figure 20 presents the server's response to this request, including detailed call records containing the contacted mobile numbers and each call's date, time, and duration.



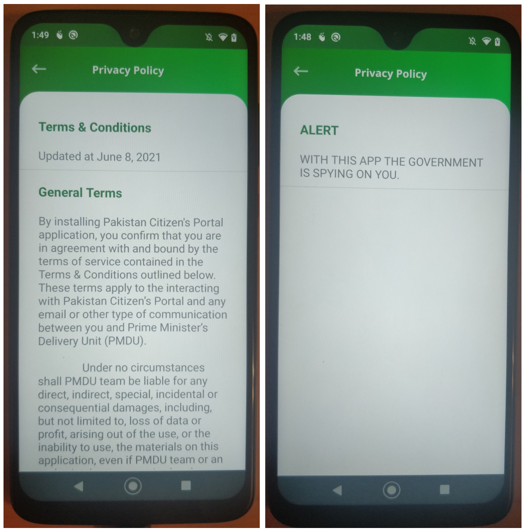
```
lake_n:/data/data/com.govpk.citizensportal/shared_prefs # cat userPref.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="userEmailcVerified">1</string>
    <int name="disability" value="0" />
    <string name="userPhoneVerified">1</string>
    <string name="userMobileVerifyTutorial">https://www.youtube.com/watch?v=MMpk-TaEBuY</string>
    <string name="blood_id">7</string>
    <string name="userDistrict"></string>
    <string name="userID">8772438</string>
    <string name="userPassportNo"></string>
    <string name="mba_provincial_listing">true</string>
    <string name="userDistrictName"></string>
    <int name="lowVision" value="0" />
    <string name="mobileVeifyAllowedToCitizen">true</string>
    <string name="userDobYear">[redacted]</string>
    <string name="profession">[redacted]</string>
    <string name="mobile_verification_feilds">1</string>
    <string name="network_title_">[redacted]</string>
    <string name="userCnic">[redacted]</string>
    <string name="userFullName">[redacted]</string>
    <string name="userProvinceId">6</string>
    <string name="userAddress">[redacted]</string>
    <string name="mba_create">true</string>
    <string name="qualification">[redacted]</string>
    <string name="network_id">5</string>
    <string name="professionID">1</string>
    <string name="userPhoto">https://cdn.pmdu.gov.pk/citizen_photos/</string>
    <string name="userProvince">[redacted]</string>
    <string name="userDistrictId">0</string>
    <string name="mobile_no">[redacted]</string>
    <string name="userCountryResidency">[redacted]</string>
    <string name="userTehsil"></string>
    <string name="userTehsilId">0</string>
    <boolean name="isLogin" value="true" />
    <string name="userDob">[redacted]</string>
    <string name="userNationality">1</string>
    <string name="userEmail">[redacted]</string>
    <string name="userDobDate">[redacted]</string>
    <string name="userDobMonth">[redacted]</string>
    <string name="show_complaint_officer_list">0</string>
    <string name="userUrduName"></string>
    <string name="userEmailVerifyTutorial">https://www.youtube.com/watch?v=dWT9T0VRt3s</string>
```

(a) PII in Android File System.

```
    <string name="userEmailVerifyTutorial">https://www.youtube.com/watch?v=dWT9T0VRt3s</string>
    <string name="qualificationID">14</string>
    <string name="userName"></string>
    <string name="religionID">1</string>
    <string name="token">eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJodHRwOlwvXC9hcGkucG1kdS5nb3YucGtcL2FwaVwvY2l0aXplbnBvcnRhbFwvdjNcL2NpdGl6ZW5cL2xvZ2luIiwiaWF0Ij
OjE3NDE2NzA1MzUsIm5iZiI6MTcxMDEzNDUzNSwianRpIjoiRDBld2JWeUJzR3huTnNENiIsInN1YiI6ODc3MjQzOCwicHJ2IjoiY2VlODczOTNiYzNmYTdkZjliNDJiODIwYThkYzczYTgyZDQwOTM2MCJ9.nS5iwpr94b
kpTLsSUvPo</string>
    <string name="religion">[redacted]</string>
    <string name="pcp_create">true</string>
    <string name="crtf_create">false</string>
    <string name="userCnicVerified">0</string>
    <int name="citizenType" value="0" />
    <string name="userCountryResidencyId">1</string>
    <string name="userGender">[redacted]</string>
    <string name="blood_grup_title">[redacted]</string>
    <string name="dataDashboard">{&quot;total&quot;:0,&quot;open&quot;:0,&quot;closed&quot;:0,&quot;postive_fb&quot;:0,&quot;negative_fb&quot;:0,&quot;pending_fb&quot;
ints&quot;:1,&quot;bubble_counts&quot;:{&quot;inbox_count&quot;:0,&quot;notification_count&quot;:0,&quot;announcement_count&quot;:16}}</string>
    <string name="landline">0</string>
</map>
```

(b) PII in Android File System (continued...).

Figure 6: PII in plaintext in Android File System for the Pakistan Citizen Portal App [62].



1:49

Privacy Policy

Terms & Conditions

Updated at June 8, 2021

General Terms

By installing Pakistan Citizen's Portal application, you confirm that you are in agreement with and bound by the terms of service contained in the Terms & Conditions outlined below. These terms apply to the interacting with Pakistan Citizen's Portal and any email or other type of communication between you and Prime Minister's Delivery Unit (PMDU).

Under no circumstances shall PMDU team be liable for any direct, indirect, special, incidental or consequential damages, including, but not limited to, loss of data or profit, arising out of the use, or the inability to use, the materials on this application, even if PMDU team or an

1:48

Privacy Policy

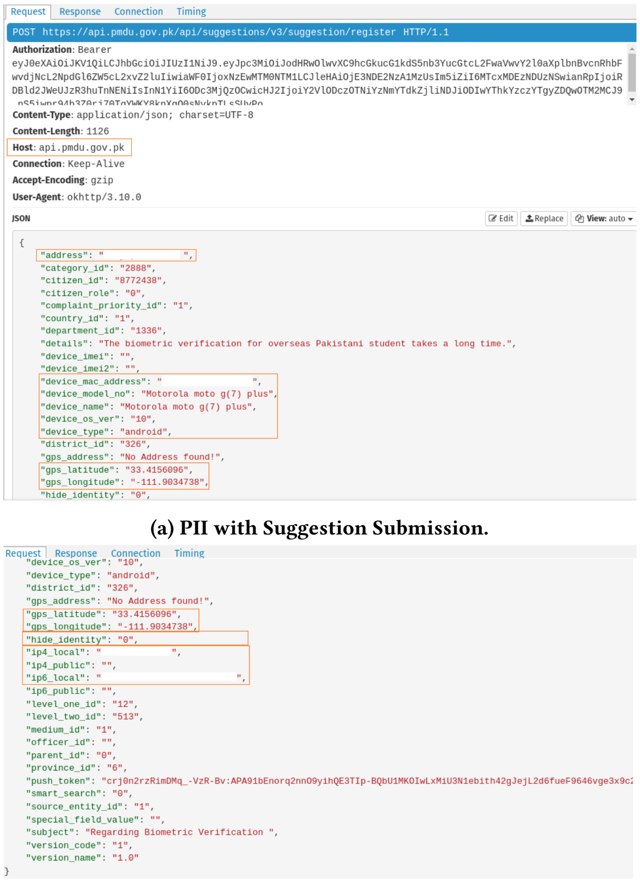
ALERT

WITH THIS APP THE GOVERNMENT IS SPYING ON YOU.

(a) Original.

(b) Spoofed.

Figure 7: Terms and Conditions in the Pakistan Citizen Portal App [62].



```
POST https://api.pmdu.gov.pk/api/suggestions/v3/suggestion/register HTTP/1.1
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJodHRwOlwvXC9hcGkucG1kdS5nb3YucGtcL2FwaVwvY2l0aXplbnBvcnRhbF
wvdjNcL2NpdGl6ZW5cL2xvZ2luIiwiaWF0IjoxNzEwMTM0NTM1LCJleHAiOjE3NDE2NzA1MzUsIm5iZiI6MTcxMDEzNDUzNSwianRpIjoiR
DBld2JWeUJzR3huTnNENiIsInN1YiI6ODc3MjQzOCwicHJ2IjoiY2VlODczOTNiYzNmYTdkZjliNDJiODIwYThkYzczYTgyZDQwOTM2MCJ9
.nS5iwpr94b37Qri7QTqYWKY8knXqQ0sNvknTLsSUvPo
Content-Type: application/json; charset=UTF-8
Content-Length: 1126
Host: api.pmdu.gov.pk
Connection: Keep-Alive
Accept-Encoding: gzip
User-Agent: okhttp/3.10.0
```

```
{
    "address": "[redacted]",
    "category_id": "2888",
    "citizen_id": "8772438",
    "citizen_role": "0",
    "complaint_priority_id": "1",
    "country_id": "1",
    "department_id": "1336",
    "details": "The biometric verification for overseas Pakistani student takes a long time.",
    "device_imei": "",
    "device_imei2": "",
    "device_mac_address": "[redacted]",
    "device_model_no": "Motorola moto g(7) plus",
    "device_name": "Motorola moto g(7) plus",
    "device_os_ver": "10",
    "device_type": "android",
    "district_id": "326",
    "gps_address": "No Address found!",
    "gps_latitude": "33.4156096",
    "gps_longitude": "-111.9034738",
    "hide_identity": "0",
```

(a) PII with Suggestion Submission.

```
    "device_os_ver": "10",
    "device_type": "android",
    "district_id": "326",
    "gps_address": "No Address found!",
    "gps_latitude": "33.4156096",
    "gps_longitude": "-111.9034738",
    "hide_identity": "0",
    "ip4_local": "[redacted]",
    "ip4_public": "",
    "ip6_local": "[redacted]",
    "ip6_public": "",
    "level_one_id": "12",
    "level_two_id": "513",
    "medium_id": "1",
    "officer_id": "",
    "parent_id": "0",
    "province_id": "6",
    "push_token": "crj0n2rzRimDMq_-VzR-Bv:APA91bEnorq2nnO9yihQE3TIp-BQbU1MKOIwLxMiU3N1ebith42gJejL2d6fueF9646vge3x9c2
    "smart_search": "0",
    "source_entity_id": "1",
    "special_field_value": "",
    "subject": "Regarding Biometric Verification ",
    "version_code": "1",
    "version_name": "1.0"
}
```

(b) PII with Suggestion Submission. (continued...).

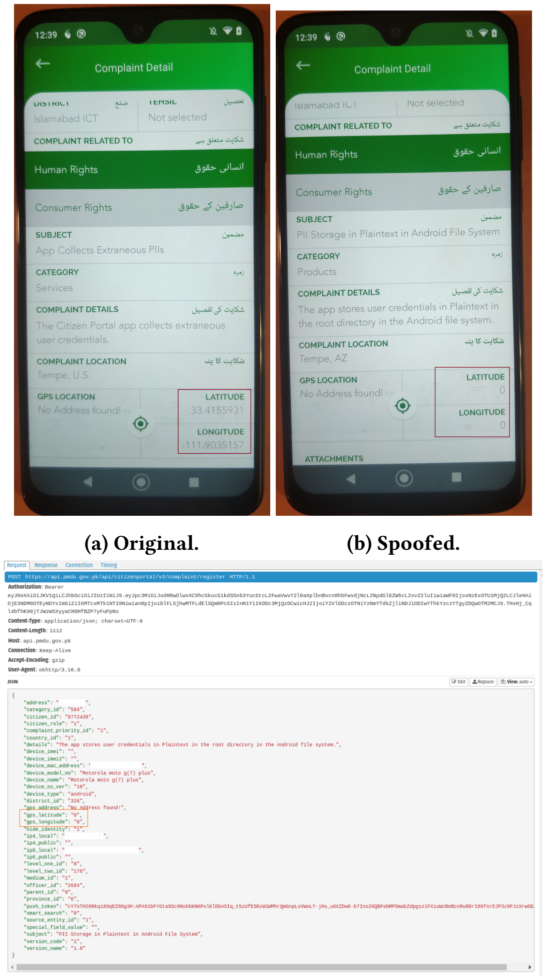
Figure 8: PII collected when submitting suggestion via the Pakistan Citizen Portal App [62].

H MY TELENOR APP

Fig. 23 and Fig. 24 illustrate that the mobile number of the user is stored in plaintext in the root directory of the Android File System for the My Telenor app [59]. In our experiment, we used two different mobile numbers, both of which were found to be stored in the root directory. Moreover, Fig. 25 shows the tax certificate generated by the My Telenor app that contains username, CNIC, and mobile number. Fig. 26 shows an at-risk user's mobile number visibility in-app traffic (in cases of compromised server private key). Fig. 27 and Fig. 28 show the call and SMS history with contacted mobile numbers, the call and SMS date, and call duration.

I UPTCL APP

Fig. 29 shows the tax certificate generated by the UPTCL app [71]. It contains the username, physical address, and the user's CNIC.



```
12:39
Complaint Detail
DISTRICT ضلع            TEHSIL تحصیل
Islamabad ICT           Not selected
COMPLAINT RELATED TO شکایت متعلق ہے
Human Rights انسانی حقوق
Consumer Rights صارفین کے حقوق
SUBJECT مضمون
App Collects Extraneous PIIs
CATEGORY زمرہ
Services
COMPLAINT DETAILS شکایت کی تفصیل
The Citizen Portal app collects extraneous
user credentials.
COMPLAINT LOCATION شکایت کا پتہ
Tempe, U.S.
GPS LOCATION            LATITUDE
No Address found!       33.4155931
                        LONGITUDE
                        -111.9035157
```

(a) Original.

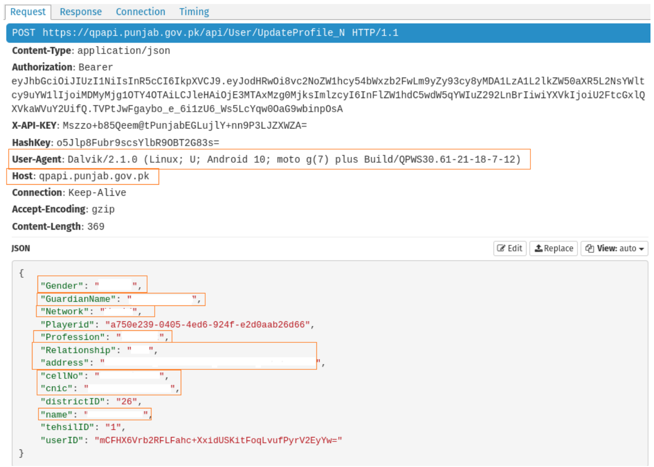
```
12:39
Complaint Detail
Islamabad ICT           Not selected
COMPLAINT RELATED TO شکایت متعلق ہے
Human Rights انسانی حقوق
Consumer Rights صارفین کے حقوق
SUBJECT مضمون
PII Storage in Plaintext in Android File System
CATEGORY زمرہ
Products
COMPLAINT DETAILS شکایت کی تفصیل
The app stores user credentials in Plaintext in
the root directory in the Android file system.
COMPLAINT LOCATION شکایت کا پتہ
Tempe, AZ
GPS LOCATION            LATITUDE
No Address found!       0
                        LONGITUDE
                        0
ATTACHMENTS
```

(b) Spoofed.

```
Request   Response   Connection   Timing
POST https://api.pmdu.gov.pk/api/citizenportal/v3/complaint/register HTTP/1.1
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJodHRwOlwvXC9hcGkucG1kdS5nb3YucGtcL2FwaVwvY2l0aXplbnBvcnRhbFwvdjNcL2NpdGl6ZW5cL2xvZ2luIiwiaWF0IjoxNzExOTU1MjQ2LCJleHAi
OjE3NDM0OTEyNDYsIm5iZiI6MTcxMTk1NTI0NiwianRpIjoiblFLSjhwMTFLdElSQmRPcSIsInN1YiI6ODc3MjQzOCwicHJ2IjoiY2VlODczOTNiYzNmYTdkZjliNDJiODIwYThkYzczYTgyZDQwOTM2MCJ9.THxHj_Cq
l4bfhK99jTJWzW5XyyaCH0HfBZP7yFuPpNs
Content-Type: application/json; charset=UTF-8
Content-Length: 1112
Host: api.pmdu.gov.pk
Connection: Keep-Alive
Accept-Encoding: gzip
User-Agent: okhttp/3.10.0
JSON                                                   Edit  Replace  View: auto
{
    "address": "[redacted]",
    "category_id": "584",
    "citizen_id": "8772438",
    "citizen_role": "1",
    "complaint_priority_id": "1",
    "country_id": "1",
    "details": "The app stores user credentials in Plaintext in the root directory in the Android file system.",
    "device_imei": "",
    "device_imei2": "",
    "device_mac_address": "[redacted]",
    "device_model_no": "Motorola moto g(7) plus",
    "device_name": "Motorola moto g(7) plus",
    "device_os_ver": "10",
    "device_type": "android",
    "district_id": "326",
    "gps_address": "No Address found!",
    "gps_latitude": "0",
    "gps_longitude": "0",
    "hide_identity": "1",
    "ip4_local": "[redacted]",
    "ip4_public": "",
    "ip6_local": "[redacted]",
    "ip6_public": "",
    "level_one_id": "8",
    "level_two_id": "176",
    "medium_id": "1",
    "officer_id": "2684",
    "parent_id": "0",
    "province_id": "6",
    "push_token": "cY7ATH20Rkqi89qEZ80g3H:APA91bFYGta9Sc9NokbKNKPolKlDbA5Iq_t5zUfESRzW1WMhrQmGnpLoVWoLY-j0o_u6XZDw6-b7Ino26QBFebMPOmabZdpgsz1FXiuWzBeBcnRuR8rI89fArEJP3z9PJzXrwGE
    "smart_search": "0",
    "source_entity_id": "1",
    "special_field_value": "",
    "subject": "PII Storage in Plaintext in Android File System",
    "version_code": "1",
    "version_name": "1.0"
}
```

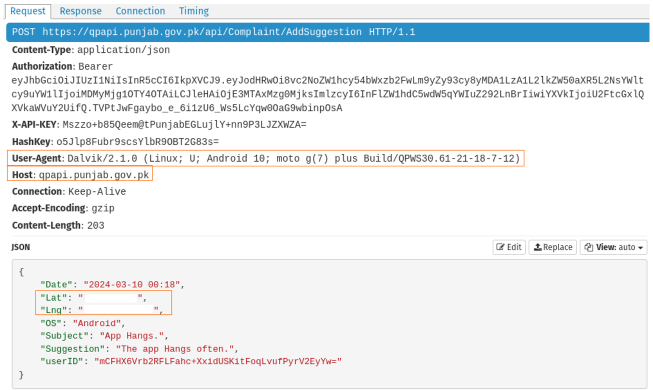
(c) Fake Location Coordinates via JSON Spoofing.

Figure 9: Location Coordinates Spoofing in the Pakistan Citizen Portal App [62].



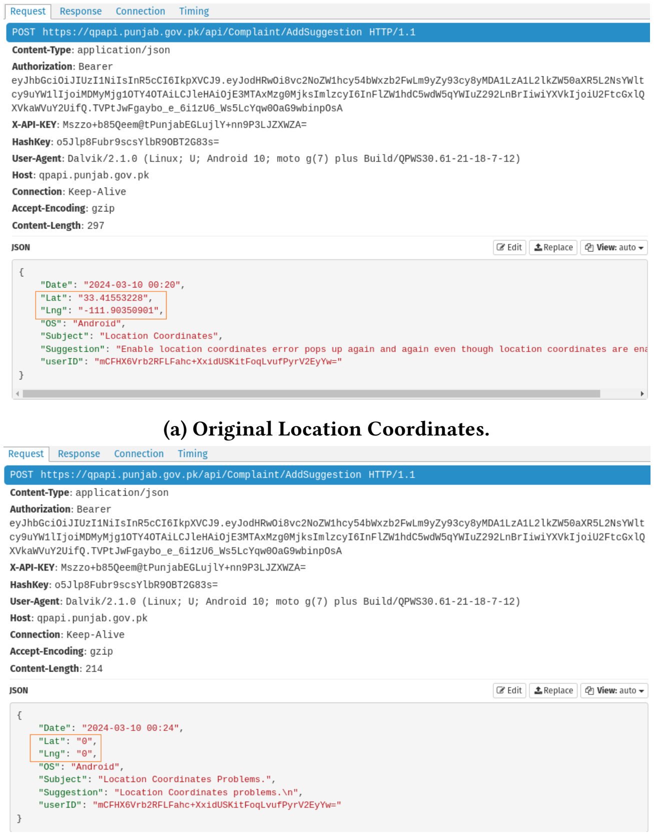
```
Request   Response   Connection   Timing
POST https://qpapi.punjab.gov.pk/api/User/UpdateProfile_N HTTP/1.1
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJodHRwOi8vc2NoZW1hcy54bWxzb2FwLm9yZy93cy8yMDA1LzA1L2lkZW50aXR5L2NsYWlt
cy9uYW1lIjoiMDMyMjg1OTY4OTAiLCJleHAiOjE3MTAxMzg0MjksImlzcyI6InFlZW1hdC5wdW5qYWIuZ292LnBrIiwiYXVkIjoiU2FtcGxlQ
XVkaWVuY2UifQ.TVPtJwFgaybo_e_6i1zU6_Ws5LcYqw0OaG9wbinpOsA
X-API-KEY: Mszzo+b85Qeem@tPunjabEGLujlY+nn9P3LJZXWZA=
HashKey: o5Jlp8Fubr9scsYlbR9OBT2G83s=
User-Agent: Dalvik/2.1.0 (Linux; U; Android 10; moto g(7) plus Build/QPWS30.61-21-18-7-12)
Host: qpapi.punjab.gov.pk
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 369
JSON                                                   Edit  Replace  View: auto
{
    "Gender": "[redacted]",
    "GuardianName": "[redacted]",
    "Network": "[redacted]",
    "Playerid": "a750e239-0405-4ed6-924f-e2d0aab26d66",
    "Profession": "[redacted]",
    "Relationship": "[redacted]",
    "address": "[redacted]",
    "cellNo": "[redacted]",
    "cnic": "[redacted]",
    "districtID": "26",
    "name": "[redacted]",
    "tehsilID": "1",
    "userID": "mCFHX6Vrb2RFLFahc+XxidUSKitFoqLvufPyrV2EyYw="
}
```

Figure 10: PII Collection for the Qeemat Punjab App [39].



```
Request   Response   Connection   Timing
POST https://qpapi.punjab.gov.pk/api/Complaint/AddSuggestion HTTP/1.1
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJodHRwOi8vc2NoZW1hcy54bWxzb2FwLm9yZy93cy8yMDA1LzA1L2lkZW50aXR5L2NsYWlt
cy9uYW1lIjoiMDMyMjg1OTY4OTAiLCJleHAiOjE3MTAxMzg0MjksImlzcyI6InFlZW1hdC5wdW5qYWIuZ292LnBrIiwiYXVkIjoiU2FtcGxlQ
XVkaWVuY2UifQ.TVPtJwFgaybo_e_6i1zU6_Ws5LcYqw0OaG9wbinpOsA
X-API-KEY: Mszzo+b85Qeem@tPunjabEGLujlY+nn9P3LJZXWZA=
HashKey: o5Jlp8Fubr9scsYlbR9OBT2G83s=
User-Agent: Dalvik/2.1.0 (Linux; U; Android 10; moto g(7) plus Build/QPWS30.61-21-18-7-12)
Host: qpapi.punjab.gov.pk
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 203
JSON                                                   Edit  Replace  View: auto
{
    "Date": "2024-03-10 00:18",
    "Lat": "[redacted]",
    "Lng": "[redacted]",
    "OS": "Android",
    "Subject": "App Hangs.",
    "Suggestion": "The app Hangs often.",
    "userID": "mCFHX6Vrb2RFLFahc+XxidUSKitFoqLvufPyrV2EyYw="
}
```

Figure 11: Location Data Collection in Qeemat Punjab App [39].



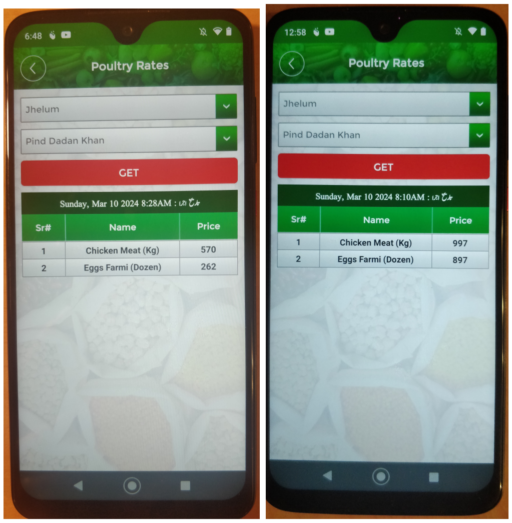
```
Request   Response   Connection   Timing
POST https://qpapi.punjab.gov.pk/api/Complaint/AddSuggestion HTTP/1.1
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJodHRwOi8vc2NoZW1hcy54bWxzb2FwLm9yZy93cy8yMDA1LzA1L2lkZW50aXR5L2NsYWlt
cy9uYW1lIjoiMDMyMjg1OTY4OTAiLCJleHAiOjE3MTAxMzg0MjksImlzcyI6InFlZW1hdC5wdW5qYWIuZ292LnBrIiwiYXVkIjoiU2FtcGxlQ
XVkaWVuY2UifQ.TVPtJwFgaybo_e_6i1zU6_Ws5LcYqw0OaG9wbinpOsA
X-API-KEY: Mszzo+b85Qeem@tPunjabEGLujlY+nn9P3LJZXWZA=
HashKey: o5Jlp8Fubr9scsYlbR9OBT2G83s=
User-Agent: Dalvik/2.1.0 (Linux; U; Android 10; moto g(7) plus Build/QPWS30.61-21-18-7-12)
Host: qpapi.punjab.gov.pk
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 297
JSON                                                   Edit  Replace  View: auto
{
    "Date": "2024-03-10 00:20",
    "Lat": "33.41553228",
    "Lng": "-111.90350901",
    "OS": "Android",
    "Subject": "Location Coordinates",
    "Suggestion": "Enable location coordinates error pops up again and again even though location coordinates are ena
    "userID": "mCFHX6Vrb2RFLFahc+XxidUSKitFoqLvufPyrV2EyYw="
}
```

(a) Original Location Coordinates.

```
Request   Response   Connection   Timing
POST https://qpapi.punjab.gov.pk/api/Complaint/AddSuggestion HTTP/1.1
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJodHRwOi8vc2NoZW1hcy54bWxzb2FwLm9yZy93cy8yMDA1LzA1L2lkZW50aXR5L2NsYWlt
cy9uYW1lIjoiMDMyMjg1OTY4OTAiLCJleHAiOjE3MTAxMzg0MjksImlzcyI6InFlZW1hdC5wdW5qYWIuZ292LnBrIiwiYXVkIjoiU2FtcGxlQ
XVkaWVuY2UifQ.TVPtJwFgaybo_e_6i1zU6_Ws5LcYqw0OaG9wbinpOsA
X-API-KEY: Mszzo+b85Qeem@tPunjabEGLujlY+nn9P3LJZXWZA=
HashKey: o5Jlp8Fubr9scsYlbR9OBT2G83s=
User-Agent: Dalvik/2.1.0 (Linux; U; Android 10; moto g(7) plus Build/QPWS30.61-21-18-7-12)
Host: qpapi.punjab.gov.pk
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 214
JSON                                                   Edit  Replace  View: auto
{
    "Date": "2024-03-10 00:24",
    "Lat": "0",
    "Lng": "0",
    "OS": "Android",
    "Subject": "Location Coordinates Problems.",
    "Suggestion": "Location Coordinates problems.\n",
    "userID": "mCFHX6Vrb2RFLFahc+XxidUSKitFoqLvufPyrV2EyYw="
}
```

(b) Spoofed Location Coordinates.

Figure 12: Planting Fake Location Coordinates via Qeemat Punjab App [39].



6:48

Poultry Rates

Jhelum

Pind Dadan Khan

GET

Sunday, Mar 10 2024 8:28AM : تاریخ اجرا

Sr#	Name	Price
1	Chicken Meat (Kg)	570
2	Eggs Farmi (Dozen)	262

(a) Original.

12:58

Poultry Rates

Jhelum

Pind Dadan Khan

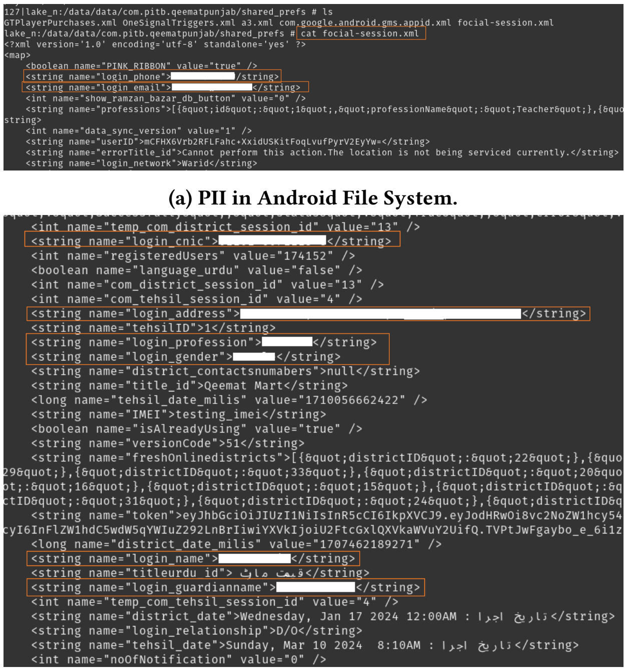
GET

Sunday, Mar 10 2024 8:10AM : تاریخ اجرا

Sr#	Name	Price
1	Chicken Meat (Kg)	997
2	Eggs Farmi (Dozen)	897

(b) Spoofed.

Figure 13: Original and Fake Prices (via JSON data spoofing) in the Qeemat Punjab App [39].



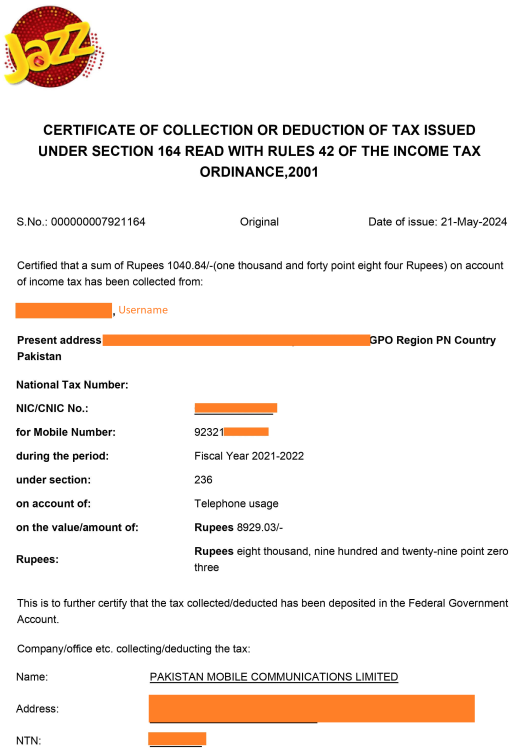
```
127|lake_n:/data/data/com.pitb.qeematpunjab/shared_prefs # ls
GTPlayerPurchases.xml OneSignalTriggers.xml a3.xml com.google.android.gms.appid.xml focial-session.xml
lake_n:/data/data/com.pitb.qeematpunjab/shared_prefs # cat focial-session.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <boolean name="PINK_RIBBON" value="true" />
    <string name="login_phone">[redacted]/string>
    <string name="login_email">[redacted]</string>
    <int name="show_ramzan_bazar_db_button" value="0" />
    <string name="professions">[{&quot;id&quot;:&quot;1&quot;,&quot;professionName&quot;:&quot;Teacher&quot;},{&quo
string>
    <int name="data_sync_version" value="1" />
    <string name="userID">mCFHX6Vrb2RFLFahc+XxidUSKitFoqLvufPyrV2EyYw=</string>
    <string name="errorTitle_id">Cannot perform this action.The location is not being serviced currently.</string>
    <string name="login_network">Warid</string>
```

(a) PII in Android File System.

```
    <int name="temp_com_district_session_id" value="13" />
    <string name="login_cnic">[redacted]</string>
    <int name="registeredUsers" value="174152" />
    <boolean name="language_urdu" value="false" />
    <int name="com_district_session_id" value="13" />
    <int name="com_tehsil_session_id" value="4" />
    <string name="login_address">[redacted]</string>
    <string name="tehsilID">1</string>
    <string name="login_profession">[redacted]</string>
    <string name="login_gender">[redacted]</string>
    <string name="district_contactsnumabers">null</string>
    <string name="title_id">Qeemat Mart</string>
    <long name="tehsil_date_milis" value="1710056662422" />
    <string name="IMEI">testing_imei</string>
    <boolean name="isAlreadyUsing" value="true" />
    <string name="versionCode">51</string>
    <string name="freshOnlinedistricts">[{&quot;districtID&quot;:&quot;22&quot;},{&quo
29&quot;},{&quot;districtID&quot;:&quot;33&quot;},{&quot;districtID&quot;:&quot;20&quo
ot;:&quot;16&quot;},{&quot;districtID&quot;:&quot;15&quot;},{&quot;districtID&quot;:&q
ctID&quot;:&quot;31&quot;},{&quot;districtID&quot;:&quot;24&quot;},{&quot;districtID&q
    <string name="token">eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJodHRwOi8vc2NoZW1hcy54
cyI6InFlZW1hdC5wdW5qYWIuZ292LnBrIiwiYXVkIjoiU2FtcGxlQXVkaWVuY2UifQ.TVPtJwFgaybo_e_6i1z
    <long name="district_date_milis" value="1707462189271" />
    <string name="login_name">[redacted]</string>
    <string name="titleurdu_id"> قیمت مارٹ</string>
    <string name="login_guardianname">[redacted]</string>
    <int name="temp_com_tehsil_session_id" value="4" />
    <string name="district_date">Wednesday, Jan 17 2024 12:00AM : تاریخ اجرا</string>
    <string name="login_relationship">D/O</string>
    <string name="tehsil_date">Sunday, Mar 10 2024  8:10AM : تاریخ اجرا</string>
    <int name="noOfNotification" value="0" />
```

(b) PII in Android File System (continued..).

Figure 14: PII storage in Plaintext for the Qeemat Punjab App [39].



CERTIFICATE OF COLLECTION OR DEDUCTION OF TAX ISSUED UNDER SECTION 164 READ WITH RULES 42 OF THE INCOME TAX ORDINANCE,2001

S.No.: 000000007921164 Original Date of issue: 21-May-2024

Certified that a sum of Rupees 1040.84/-(one thousand and forty point eight four Rupees) on account of income tax has been collected from:

[redacted], Username

Present address [redacted] **GPO Region PN Country Pakistan**

National Tax Number:

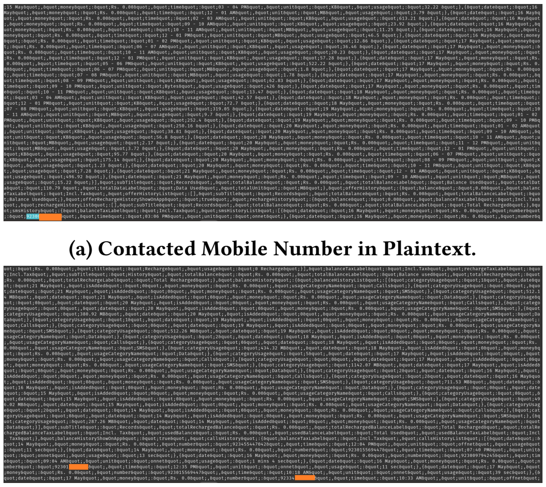
NIC/CNIC No.:	[redacted]
for Mobile Number:	92321[redacted]
during the period:	Fiscal Year 2021-2022
under section:	236
on account of:	Telephone usage
on the value/amount of:	**Rupees** 8929.03/-
Rupees:	**Rupees** eight thousand, nine hundred and twenty-nine point zero three

This is to further certify that the tax collected/deducted has been deposited in the Federal Government Account.

Company/office etc. collecting/deducting the tax:

Name:	PAKISTAN MOBILE COMMUNICATIONS LIMITED
Address:	[redacted]
NTN:	[redacted]

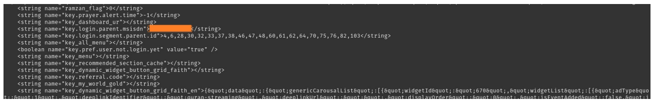
Figure 15: Tax Certificate generated by the SIMOSA App [68].



(a) Contacted Mobile Number in Plaintext.

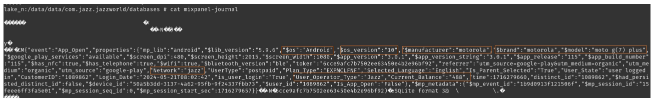
(b) Contacted Mobile Numbers in Plaintext.

Figure 16: Call and SMS History for the SIMOSA App [68].



```
    <string name="ramzan_flag">0</string>
    <string name="key.prayer.alert.time">-1</string>
    <string name="key_dashboard_ur"></string>
    <string name="key.login.parent.msisdn">[redacted]</string>
    <string name="key.login.segment.parent.id">4,6,28,30,32,33,37,38,46,47,48,60,61,62,64,70,75,76,82,103</string>
    <string name="key_all_menu"></string>
    <boolean name="key.pref.user.not.login.yet" value="true" />
    <string name="key_menu"></string>
    <string name="key_recommended_section_cache"></string>
    <string name="key_dynamic_widget_button_grid_faith"></string>
    <string name="key.referral.code"></string>
    <string name="key_my_world_gold"></string>
    <string name="key_dynamic_widget_button_grid_faith_en">{&quot;data&quot;:{&quot;genericCarousalList&quot;:[{&quot;widgetId&quot;:&quot;670&quot;,&quot;widgetList&quot;:[{&quot;adType&quo
t;:&quot;1&quot;,&quot;deeplinkIdentifier&quot;:&quot;quran-streaming&quot;,&quot;deeplinkUrl&quot;:&quot;&quot;,&quot;displayOrder&quot;:&quot;0&quot;,&quot;isEventAdded&quot;:false,&quot;i
```

Figure 17: PII in plaintext in the Android File System for the SIMOSA App [68].

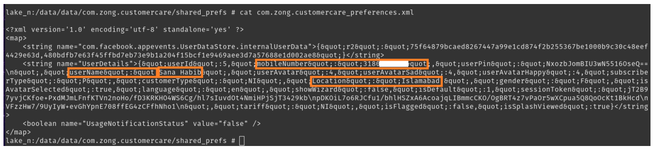


```
lake_n:/data/data/com.jazz.jazzworld/databases # cat mixpanel-journal

������                               �
                                       ��N��)��

y�
���CM{"event":"App_Open","properties":{"mp_lib":"android","$lib_version":"5.9.6","$os":"Android","$os_version":"10","$manufacturer":"motorola","$brand":"motorola","$model":"moto g(7) plus",
"$google_play_services":"available","$screen_dpi":480,"$screen_height":2015,"$screen_width":1080,"$app_version":"3.0.1","$app_version_string":"3.0.1","$app_release":"115","$app_build_number"
:"115","$has_nfc":true,"$has_telephone":true,"$wifi":true,"$bluetooth_version":"ble","token":"6cce9afc7b7502ee63450e4b2e96bf92","referrer":"utm_source=google-play&utm_medium=organic","utm_me
dium":"organic","utm_source":"google-play","Network":"jazz","UserType":"postpaid","Plan_Type":"EXPMCLFNF","Selected_Language":"English","Is_Parent_Selected":"True","User_State":"user logged
in","CustomerID":"1089862","Login_Date":"2024-05-21T08:02:42","is_user_login":"True","User_Operator_Type":"Jazz","Current_Balance":"488","time":1716279660,"distinct_id":"1089862","$had_persi
sted_distinct_id":false,"$device_id":"50a5b3dd-3137-4a62-95fb-9f24337fbb73","$user_id":"1089862","Is_App_Open":"False"},"$mp_metadata":{"$mp_event_id":"1b9d0913f121506f","$mp_session_id":"15
feee6ff3fa5e01","$mp_session_seq_id":0,"$mp_session_start_sec":1716279657}}��N�6cce9afc7b7502ee63450e4b2e96bf92)�SQLite format 3@  \         \.�
����
```

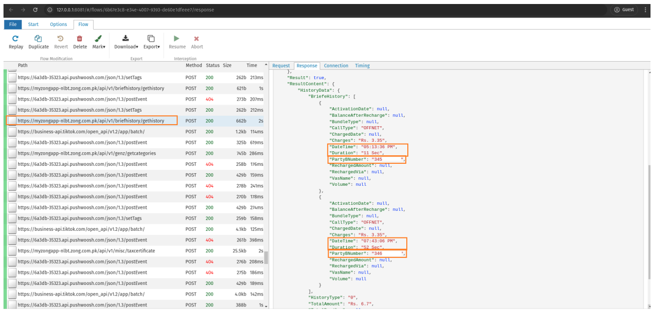
Figure 18: Device details in plaintext in the Android File System for the SIMOSA App [68].



```
lake_n:/data/data/com.zong.customercare/shared_prefs # cat com.zong.customercare_preferences.xml

<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="com.facebook.appevents.UserDataStore.internalUserData">{&quot;r2&quot;:&quot;75f64879bcaed8267447a99e1cd874f2b255367be1000b9c30c48eef
4429e63d,480bdfb7e63f45ffbd7eb73e9b1a204f15bcf1e9469aee3d7a57688e1d002ae8&quot;}</string>
    <string name="UserDetails">{&quot;userId&quot;:5,&quot;mobileNumber&quot;:&quot;3180[redacted]&quot;,&quot;userPin&quot;:&quot;NxozbJomBIU3wN5516OseQ==
\n&quot;,&quot;userName&quot;:&quot; Sana Habib&quot;,&quot;userAvatar&quot;:4,&quot;userAvatarSad&quot;:4,&quot;userAvatarHappy&quot;:4,&quot;subscribe
rType&quot;:&quot;P&quot;,&quot;customerType&quot;:&quot;NI&quot;,&quot;Location&quot;:&quot;Islamabad &quot;,&quot;gender&quot;:&quot;F&quot;,&quot;is
AvatarSelected&quot;:true,&quot;language&quot;:&quot;en&quot;,&quot;showWizard&quot;:false,&quot;isDefault&quot;:1,&quot;sessionToken&quot;:&quot;jT2B9
7yvjCKfoe+PxdMJmLFnfKTVn2noHo/fD3KRKHO4WS6Cg/hl7sIuvdOt4NmiHPjSjT3429kb\npDKOiL7o6RJCfu1/bhlHSZxA6AcoajqLIBmmcCKO/OgBRT4z7vPaOr5wXCpua5Q8QoOcKt1BkHcd\n
VFzzHw7/9UyIyW+evGhYpnE708ffEG4zCFfhNho1\n&quot;,&quot;tariff&quot;:&quot;NI&quot;,&quot;isFlagged&quot;:false,&quot;isSplashViewed&quot;:true}</string
>
    <boolean name="UsageNotificationStatus" value="false" />
</map>
lake_n:/data/data/com.zong.customercare/shared_prefs # 
```

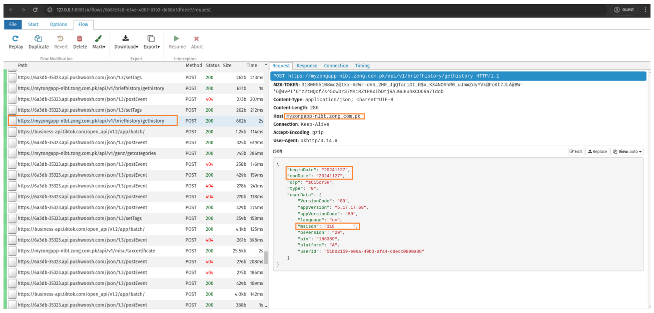
Figure 19: PII in plaintext in the Android File System for My Zong App [59].



Path	Method	Status	Size	Time
https://6a3db-35323.api.pushwoosh.com/json/1.3/setTags	POST	200	262b	213ms
https://myzongapp-nlbt.zong.com.pk/api/v1/briefhistory/gethistory	POST	200	621b	1s
https://6a3db-35323.api.pushwoosh.com/json/1.3/postEvent	POST	404	273b	207ms
https://6a3db-35323.api.pushwoosh.com/json/1.3/setTags	POST	200	262b	212ms
https://myzongapp-nlbt.zong.com.pk/api/v1/briefhistory/gethistory	POST	200	662b	2s
https://business-api.tiktok.com/open_api/v1.2/app/batch/	POST	200	1.2kb	114ms
https://6a3db-35323.api.pushwoosh.com/json/1.3/postEvent	POST	200	325b	619ms
https://myzongapp-nlbt.zong.com.pk/api/v1/genz/getcategories	POST	200	745b	286ms
https://6a3db-35323.api.pushwoosh.com/json/1.3/postEvent	POST	404	258b	176ms
https://6a3db-35323.api.pushwoosh.com/json/1.3/postEvent	POST	200	429b	159ms
https://6a3db-35323.api.pushwoosh.com/json/1.3/postEvent	POST	404	278b	241ms
https://6a3db-35323.api.pushwoosh.com/json/1.3/postEvent	POST	404	270b	178ms
https://6a3db-35323.api.pushwoosh.com/json/1.3/postEvent	POST	200	429b	274ms
https://6a3db-35323.api.pushwoosh.com/json/1.3/setTags	POST	200	259b	158ms
https://business-api.tiktok.com/open_api/v1.2/app/batch/	POST	200	4.1kb	125ms
https://6a3db-35323.api.pushwoosh.com/json/1.3/postEvent	POST	404	261b	398ms
https://myzongapp-nlbt.zong.com.pk/api/v1/misc/taxcertificate	POST	200	25.5kb	2s
https://6a3db-35323.api.pushwoosh.com/json/1.3/postEvent	POST	404	276b	208ms
https://6a3db-35323.api.pushwoosh.com/json/1.3/postEvent	POST	404	275b	186ms
https://6a3db-35323.api.pushwoosh.com/json/1.3/postEvent	POST	200	429b	189ms
https://business-api.tiktok.com/open_api/v1.2/app/batch/	POST	200	4.0kb	142ms
https://6a3db-35323.api.pushwoosh.com/json/1.3/postEvent	POST	200	388b	1s

```
    },
    "Result": true,
    "ResultContent": {
        "HistoryData": {
            "BriefeHistory": [
                {
                    "ActivationDate": null,
                    "BalanceAfterRecharge": null,
                    "BundleType": null,
                    "CallType": "OFFNET",
                    "ChargedDate": null,
                    "Charges": "Rs. 3.35",
                    "DateTime": "05:13:36 PM",
                    "Duration": "11 Sec",
                    "PartyBNumber": "345[redacted]",
                    "RechargedAmount": null,
                    "RechargedVia": null,
                    "VasName": null,
                    "Volume": null
                },
                {
                    "ActivationDate": null,
                    "BalanceAfterRecharge": null,
                    "BundleType": null,
                    "CallType": "OFFNET",
                    "ChargedDate": null,
                    "Charges": "Rs. 3.35",
                    "DateTime": "07:43:06 PM",
                    "Duration": "52 Sec",
                    "PartyBNumber": "346[redacted]",
                    "RechargedAmount": null,
                    "RechargedVia": null,
                    "VasName": null,
                    "Volume": null
                }
            ],
            "HistoryType": "0",
            "TotalAmount": "Rs. 6.7",
```

Figure 20: Call/SMS Records for the My Zong App [59].

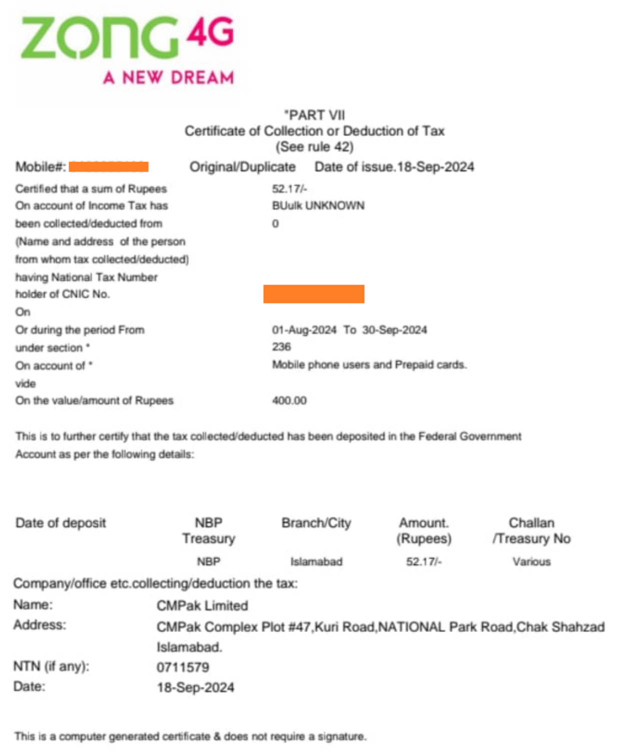


Path	Method	Status	Size	Time
https://6a3db-35323.api.pushwoosh.com/json/1.3/setTags	POST	200	262b	213ms
https://myzongapp-nlbt.zong.com.pk/api/v1/briefhistory/gethistory	POST	200	621b	1s
https://6a3db-35323.api.pushwoosh.com/json/1.3/postEvent	POST	404	273b	207ms
https://6a3db-35323.api.pushwoosh.com/json/1.3/setTags	POST	200	262b	212ms
https://myzongapp-nlbt.zong.com.pk/api/v1/briefhistory/gethistory	POST	200	662b	2s
https://business-api.tiktok.com/open_api/v1.2/app/batch/	POST	200	1.2kb	114ms
https://6a3db-35323.api.pushwoosh.com/json/1.3/postEvent	POST	200	325b	619ms
https://myzongapp-nlbt.zong.com.pk/api/v1/genz/getcategories	POST	200	745b	286ms
https://6a3db-35323.api.pushwoosh.com/json/1.3/postEvent	POST	404	258b	176ms
https://6a3db-35323.api.pushwoosh.com/json/1.3/postEvent	POST	200	429b	159ms
https://6a3db-35323.api.pushwoosh.com/json/1.3/postEvent	POST	404	278b	241ms
https://6a3db-35323.api.pushwoosh.com/json/1.3/postEvent	POST	404	270b	178ms
https://6a3db-35323.api.pushwoosh.com/json/1.3/postEvent	POST	200	429b	274ms
https://6a3db-35323.api.pushwoosh.com/json/1.3/setTags	POST	200	259b	158ms
https://business-api.tiktok.com/open_api/v1.2/app/batch/	POST	200	4.1kb	125ms
https://6a3db-35323.api.pushwoosh.com/json/1.3/postEvent	POST	404	261b	398ms
https://myzongapp-nlbt.zong.com.pk/api/v1/misc/taxcertificate	POST	200	25.5kb	2s
https://6a3db-35323.api.pushwoosh.com/json/1.3/postEvent	POST	404	276b	208ms
https://6a3db-35323.api.pushwoosh.com/json/1.3/postEvent	POST	404	275b	186ms
https://6a3db-35323.api.pushwoosh.com/json/1.3/postEvent	POST	200	429b	189ms
https://business-api.tiktok.com/open_api/v1.2/app/batch/	POST	200	4.0kb	142ms
https://6a3db-35323.api.pushwoosh.com/json/1.3/postEvent	POST	200	388b	1s

```
POST https://myzongapp-nlbt.zong.com.pk/api/v1/briefhistory/gethistory HTTP/1.1
MZA-TOKEN: 3180055108mc2@tkx-#mWr-d#h_2H0_JgQTariGt_R$x_KX4NO#hR0_uJnmZdyYVk@FoKt7JLA@8W-
*6@4vPI*6*z2tHQcfZs^5owDr37M#1RZ1PBxIbDtjRAJGuHuhKCO6Ra7Tdob
Content-Type: application/json; charset=UTF-8
Content-Length: 286
Host: myzongapp-nlbt.zong.com.pk
Connection: Keep-Alive
Accept-Encoding: gzip
User-Agent: okhttp/3.14.9

JSON
{
    "beginDate": "20241127",
    "endDate": "20241127",
    "oTp": "zC15cr3H",
    "type": "0",
    "userData": {
        "VersionCode": "89",
        "appVersion": "5.17.17.68",
        "appVersionCode": "89",
        "language": "en",
        "msisdn": "318[redacted]",
        "osVersion": "29",
        "pin": "186389",
        "platform": "A",
        "userId": "51bd2159-e06a-49b3-afa4-cdecc0890a88"
    }
}
```

Figure 21: Mobile Number Visibility in the My Zong App [59].



ZONG 4G
A NEW DREAM

"PART VII
Certificate of Collection or Deduction of Tax
(See rule 42)

Mobile#: [redacted] Original/Duplicate Date of issue.18-Sep-2024

Certified that a sum of Rupees	52.17/-
On account of Income Tax has	BUulk UNKNOWN
been collected/deducted from	0
(Name and address of the person	
from whom tax collected/deducted)	
having National Tax Number	
holder of CNIC No.	[redacted]
On	
Or during the period From	01-Aug-2024 To 30-Sep-2024
under section *	236
On account of *	Mobile phone users and Prepaid cards.
vide	
On the value/amount of Rupees	400.00

This is to further certify that the tax collected/deducted has been deposited in the Federal Government Account as per the following details:

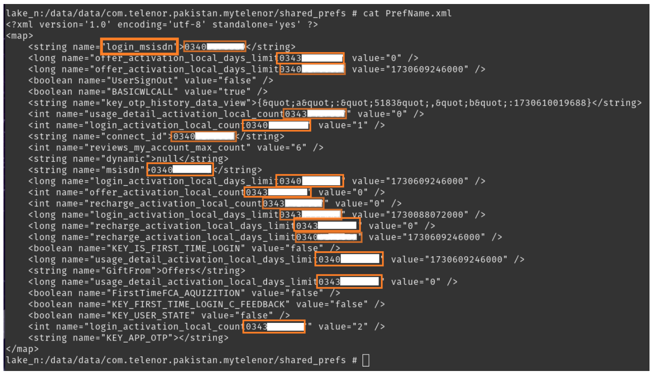
Date of deposit	NBP Treasury	Branch/City	Amount. (Rupees)	Challan /Treasury No
	NBP	Islamabad	52.17/-	Various

Company/office etc.collecting/deduction the tax:

Name:	CMPak Limited
Address:	CMPak Complex Plot #47,Kuri Road,NATIONAL Park Road,Chak Shahzad Islamabad.
NTN (if any):	0711579
Date:	18-Sep-2024

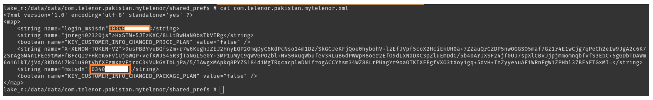
This is a computer generated certificate & does not require a signature.

Figure 22: Tax Certificate generated by the My Zong App [59].



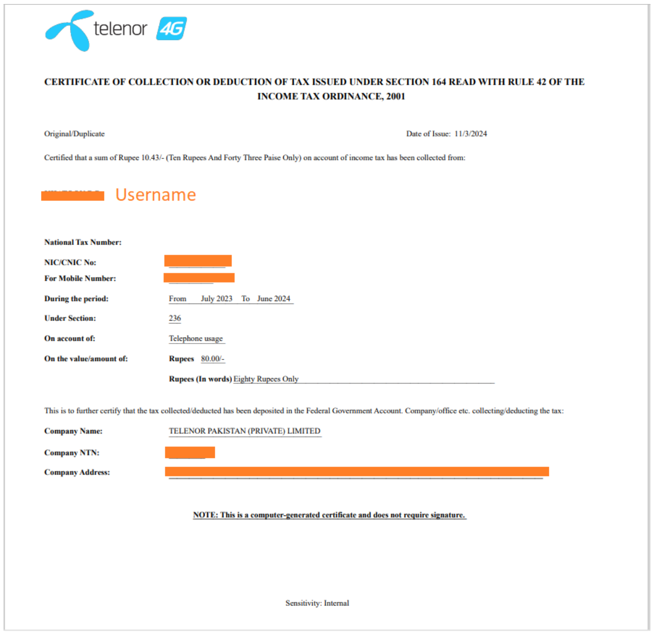
```
lake_n:/data/data/com.telenor.pakistan.mytelenor/shared_prefs # cat PrefName.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="login_msisdn">0340[redacted]</string>
    <long name="offer_activation_local_days_limit0343[redacted] value="0" />
    <long name="offer_activation_local_days_limit0340[redacted] value="1730609246000" />
    <boolean name="UserSignOut" value="false" />
    <boolean name="BASICWLCALL" value="true" />
    <string name="key_otp_history_data_view">{&quot;a&quot;:&quot;5183&quot;,&quot;b&quot;:1730610019688}</string>
    <int name="usage_detail_activation_local_count0343[redacted]" value="0" />
    <int name="login_activation_local_count0340[redacted] value="1" />
    <string name="connect_id">0340[redacted]</string>
    <int name="reviews_my_account_max_count" value="6" />
    <string name="dynamic">null</string>
    <string name="msisdn">0340[redacted]</string>
    <long name="login_activation_local_days_limit0340[redacted] value="1730609246000" />
    <int name="offer_activation_local_count0343[redacted] value="0" />
    <int name="recharge_activation_local_count0343[redacted]" value="0" />
    <long name="login_activation_local_days_limit0343[redacted]" value="1730088072000" />
    <long name="recharge_activation_local_days_limit0343[redacted] value="0" />
    <long name="recharge_activation_local_days_limit0340[redacted] value="1730609246000" />
    <boolean name="KEY_IS_FIRST_TIME_LOGIN" value="false" />
    <long name="usage_detail_activation_local_days_limit0340[redacted] value="1730609246000" />
    <string name="GiftFrom">Offers</string>
    <long name="usage_detail_activation_local_days_limit0343[redacted] value="0" />
    <boolean name="FirstTimeFCA_AQUIZITION" value="false" />
    <boolean name="KEY_FIRST_TIME_LOGIN_C_FEEDBACK" value="false" />
    <boolean name="KEY_USER_STATE" value="false" />
    <int name="login_activation_local_count0343[redacted]" value="2" />
    <string name="KEY_APP_OTP"></string>
</map>
lake_n:/data/data/com.telenor.pakistan.mytelenor/shared_prefs # 
```

Figure 23: PII in plaintext in the Android File System for My Telenor App [58].



```
lake_n:/data/data/com.telenor.pakistan.mytelenor/shared_prefs # cat com.telenor.pakistan.mytelenor.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="login_msisdn">0340[redacted]</string>
    <string name="jnregi02320js">HxSTM+5JIzKXC/8LLtBwHaN0bsTkVIRg</string>
    <boolean name="KEY_CUSTOMER_INFO_CHANGED_PRICE_PLAN" value="false" />
    <string name="X-XENON-TOKEN-V2">9usPBBYvuBQfsZm+r7w6KeghJZEJ2HnyEQP2OmqDyC6KdPcNso14m1DZ/SkGCJeKFjQoe0hybohV+lzEfJVpf5coX2HciEkUH0a+7ZZauQrCZDP5nwOGGSO5maf7Gz1r4E1wCjg7qPeCh2eIw9JgA2c6K7
ZSrAgGM4n1FEe9tMwFfBFcQIrFHkeK6FviUjGWQP+vefKWJS45R3jTaNGL5e0Y+3MP1uMyC9qWVGPOZbl+NVS0xuqWbufeV3RLuB6dPWWpR8oer2EfO9dLxNaDXC3pZluEmDdC/5b40ArJXSF24jf0UJ7spXlCBVJjpjmmomnqbfvfS3EbC+5gGDbTDAWm
6o161kI/jVd/3KDdAi7k6lu90tVhfXEgmxavEtroC34VUkGsIbLjPa/5/IAwgxMApkq8PYZS184d1MgTRqcacplwDN1frogACCYhsm34WZ88LrPUagYr9oaOTKIXEEgfVXO3tXoy1gq+5dvH+InZyye4uAF1WRnFgW1ZPHbl37BE4FTGxMI=</string>
    <string name="msisdn">0340[redacted]</string>
    <boolean name="KEY_CUSTOMER_INFO_CHANGED_PACKAGE_PLAN" value="false" />
</map>
lake_n:/data/data/com.telenor.pakistan.mytelenor/shared_prefs # 
```

Figure 24: PII in plaintext in the Android File System for My Telenor App [58].



CERTIFICATE OF COLLECTION OR DEDUCTION OF TAX ISSUED UNDER SECTION 164 READ WITH RULE 42 OF THE INCOME TAX ORDINANCE, 2001

Original/Duplicate Date of Issue: 11/3/2024

Certified that a sum of Rupee 10.43/- (Ten Rupees And Forty Three Paise Only) on account of income tax has been collected from:

[redacted] Username

National Tax Number:	
NIC/CNIC No:	[redacted]
For Mobile Number:	[redacted]
During the period:	From July 2023 To June 2024
Under Section:	236
On account of:	Telephone usage
On the value/amount of:	**Rupees** 80.00/-
	Rupees (In words) Eighty Rupees Only

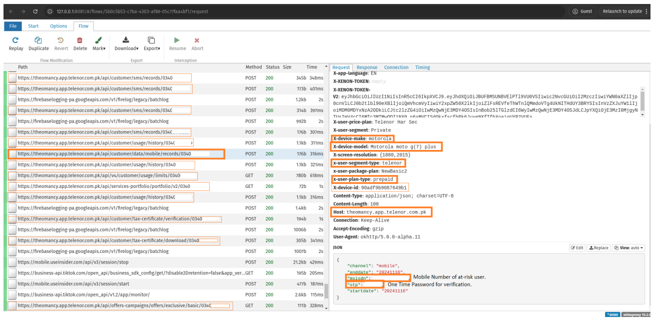
This is to further certify that the tax collected/deducted has been deposited in the Federal Government Account. Company/office etc. collecting/deducting the tax:

Company Name:	TELENOR PAKISTAN (PRIVATE) LIMITED
Company NTN:	[redacted]
Company Address:	[redacted]

NOTE: This is a computer-generated certificate and does not require signature.

Sensitivity: Internal

Figure 25: Tax Certificate generated by the My Telenor App [58].



```
Path                                                                                        Method Status Size  Time
https://theomancy.app.telenor.com.pk/api/customer/sms/records/0340                          POST   200    345b  348ms
https://theomancy.app.telenor.com.pk/api/customer/sms/records/034[redacted]                 POST   200    173b  401ms
https://firebaselogging-pa.googleapis.com/v1/firelog/legacy/batchlog                        POST   200    1.2kb 2s
https://theomancy.app.telenor.com.pk/api/customer/sms/records/034[redacted]                 POST   200    314b  397ms
https://firebaselogging-pa.googleapis.com/v1/firelog/legacy/batchlog                        POST   200    992b  2s
https://theomancy.app.telenor.com.pk/api/customer/sms/records/034[redacted]                 POST   200    176b  307ms
https://theomancy.app.telenor.com.pk/api/customer/usage/history/034[redacted]               POST   200    1.1kb 311ms
https://theomancy.app.telenor.com.pk/api/customer/data/mobile/records/0340[redacted]        POST   200    176b  316ms
https://theomancy.app.telenor.com.pk/api/customer/usage/history/0340                        POST   200    1.1kb 321ms
https://theomancy.app.telenor.com.pk/api/v4/customer/usage/limits/0340[redacted]            GET    200    780b  618ms
https://theomancy.app.telenor.com.pk/api/services-portfolio/portfolio/v2/0340               GET    200    72b   1s
https://theomancy.app.telenor.com.pk/api/customer/usage/history/034[redacted]               POST   200    1.1kb 316ms
https://firebaselogging-pa.googleapis.com/v1/firelog/legacy/batchlog                        POST   200    1.4kb 2s
https://theomancy.app.telenor.com.pk/api/customer/tax-certificate/verification/0340         POST   200    194b  1s
https://firebaselogging-pa.googleapis.com/v1/firelog/legacy/batchlog                        POST   200    1006b 2s
https://theomancy.app.telenor.com.pk/api/customer/tax-certificate/download/0340[redacted]   POST   200    305b  341ms
https://firebaselogging-pa.googleapis.com/v1/firelog/legacy/batchlog                        POST   200    1007b 2s
https://mobile.useinsider.com/api/v3/session/stop                                           POST   200    21.2kb 429ms
https://business-api.tiktok.com/open_api/business_sdk_config/get/?disable2Dretention=false&app_ver...GET 200 195b 205ms
https://mobile.useinsider.com/api/v3/session/start                                          POST   200    477b  187ms
https://business-api.tiktok.com/open_api/v1.2/app/monitor/                                  POST   200    2.6kb 115ms
https://theomancy.app.telenor.com.pk/api/offers-campaigns/offers/exclusive/basic/034[redacted] GET  200    111b  328ms
```

```
X-app-language: EN
X-XENON-TOKEN: empty
X-XENON-TOKEN-V2: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhdXQiOiJBUFBMSUNBVElPTl9VU0VSIiwic2NvcGUiOiI2MzczIiwiYWN0aXZlIjp0cnVlLCJ0b2tlbl90eXBlIjoiQmVhcmVyIiwiY2xpZW50X2lkIjoiZlFsREVfeThWTnlQMmdoVTg4UkNITHdUY3BRYSIsInVzZXJuYW1lIjoiMDM0MDYxNzA2ODkiLCJtc2lzZG4iOiIwMzQwNjE3MDY4OSIsInBob25lTGlzdCI6WyIwMzQwNjE3MDY4OSJdLCJpYXQiOjE3MzI0MjgyNTUsImV4cCI6MTc3MTMwODI1NX0.n6sMVCISdOkxfscfbPk6JuveNXfTfbXoaiqUYR2VUEs
X-user-price-plan: Telenor Har Sec
X-user-segment: Private
X-device-make: motorola
X-device-model: Motorola moto g(7) plus
X-screen-resolution: {1080,2015}
x-user-segment-type: telenor
x-user-package-plan: NewBasic2
x-user-plan-type: prepaid
X-device-id: 90adf9b9087649b1
Content-Type: application/json; charset=UTF-8
Content-Length: 100
Host: theomancy.app.telenor.com.pk
Connection: Keep-Alive
Accept-Encoding: gzip
User-Agent: okhttp/5.0.0-alpha.11
```

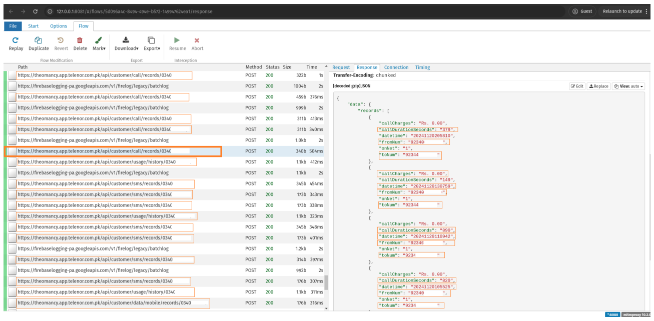
JSON

```
{
    "channel": "mobile",
    "enddate": "20241116",
    "msisdn": [redacted],
    "otp": [redacted],
    "startdate": "20241116"
}
```

Mobile Number of at-risk user.

One Time Password for verification.

Figure 26: Mobile Number Visibility in My Telenor App [58].



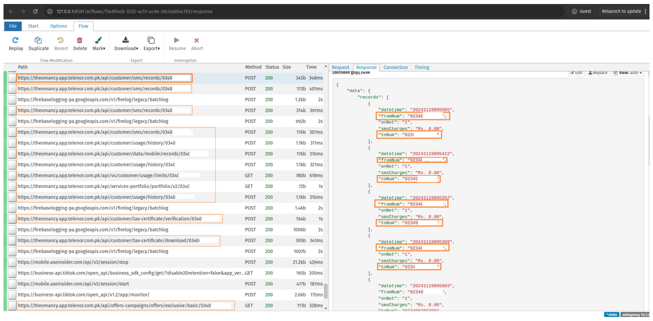
```
Path                                                                                     Method Status Size  Time
https://theomancy.app.telenor.com.pk/api/customer/call/records/0340                      POST   200    322b  1s
https://firebaselogging-pa.googleapis.com/v1/firelog/legacy/batchlog                     POST   200    1004b 2s
https://theomancy.app.telenor.com.pk/api/customer/call/records/034[redacted]             POST   200    459b  376ms
https://firebaselogging-pa.googleapis.com/v1/firelog/legacy/batchlog                     POST   200    999b  2s
https://theomancy.app.telenor.com.pk/api/customer/call/records/0340                      POST   200    311b  413ms
https://theomancy.app.telenor.com.pk/api/customer/call/records/034[redacted]             POST   200    311b  340ms
https://firebaselogging-pa.googleapis.com/v1/firelog/legacy/batchlog                     POST   200    1.0kb 2s
https://theomancy.app.telenor.com.pk/api/customer/call/records/034[redacted]             POST   200    340b  504ms
https://theomancy.app.telenor.com.pk/api/customer/usage/history/0340                     POST   200    1.1kb 412ms
https://firebaselogging-pa.googleapis.com/v1/firelog/legacy/batchlog                     POST   200    1.1kb 2s
https://theomancy.app.telenor.com.pk/api/customer/sms/records/0340                       POST   200    345b  454ms
https://theomancy.app.telenor.com.pk/api/customer/sms/records/034[redacted]              POST   200    173b  343ms
https://theomancy.app.telenor.com.pk/api/customer/sms/records/034[redacted]              POST   200    173b  338ms
https://theomancy.app.telenor.com.pk/api/customer/usage/history/034[redacted]            POST   200    1.1kb 323ms
https://theomancy.app.telenor.com.pk/api/customer/sms/records/034[redacted]              POST   200    345b  348ms
https://theomancy.app.telenor.com.pk/api/customer/sms/records/034[redacted]              POST   200    173b  401ms
https://firebaselogging-pa.googleapis.com/v1/firelog/legacy/batchlog                     POST   200    1.2kb 2s
https://theomancy.app.telenor.com.pk/api/customer/sms/records/0340[redacted]             POST   200    314b  397ms
https://firebaselogging-pa.googleapis.com/v1/firelog/legacy/batchlog                     POST   200    992b  2s
https://theomancy.app.telenor.com.pk/api/customer/sms/records/0340[redacted]             POST   200    176b  307ms
https://theomancy.app.telenor.com.pk/api/customer/usage/history/034[redacted]            POST   200    1.1kb 311ms
https://theomancy.app.telenor.com.pk/api/customer/data/mobile/records/0340[redacted]     POST   200    176b  316ms
```

Transfer-Encoding: chunked

[decoded gzip] JSON

```
{
    "data": {
        "records": [
            {
                "callCharges": "Rs. 0.00",
                "callDurationSeconds": "379",
                "datetime": "20241120205810",
                "fromNum": "92340[redacted]",
                "onNet": "1",
                "toNum": "92344[redacted]"
            },
            {
                "callCharges": "Rs. 0.00",
                "callDurationSeconds": "149",
                "datetime": "20241120130759",
                "fromNum": "92340[redacted]",
                "onNet": "1",
                "toNum": "92344[redacted]"
            },
            {
                "callCharges": "Rs. 0.00",
                "callDurationSeconds": "890",
                "datetime": "20241120110942",
                "fromNum": "92340[redacted]",
                "onNet": "1",
                "toNum": "9234[redacted]"
            },
            {
                "callCharges": "Rs. 0.00",
                "callDurationSeconds": "820",
                "datetime": "20241120105525",
                "fromNum": "92340[redacted]",
                "onNet": "1",
                "toNum": "9234[redacted]"
```

Figure 27: Call Records for the My Telenor App [58].

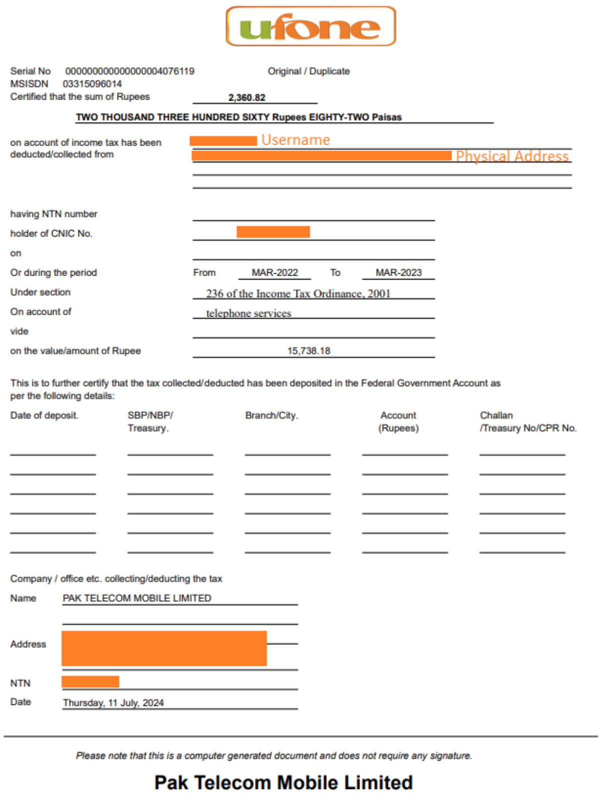


```
Path                                                                                        Method Status Size  Time
https://theomancy.app.telenor.com.pk/api/customer/sms/records/0340[redacted]                POST   200    345b  348ms
https://theomancy.app.telenor.com.pk/api/customer/sms/records/0340[redacted]                POST   200    173b  401ms
https://firebaselogging-pa.googleapis.com/v1/firelog/legacy/batchlog                        POST   200    1.2kb 2s
https://theomancy.app.telenor.com.pk/api/customer/sms/records/0340[redacted]                POST   200    314b  397ms
https://firebaselogging-pa.googleapis.com/v1/firelog/legacy/batchlog                        POST   200    992b  2s
https://theomancy.app.telenor.com.pk/api/customer/sms/records/0340[redacted]                POST   200    176b  307ms
https://theomancy.app.telenor.com.pk/api/customer/usage/history/0340                        POST   200    1.1kb 311ms
https://theomancy.app.telenor.com.pk/api/customer/data/mobile/records/034[redacted]         POST   200    176b  316ms
https://theomancy.app.telenor.com.pk/api/customer/usage/history/034                         POST   200    1.1kb 321ms
https://theomancy.app.telenor.com.pk/api/v4/customer/usage/limits/034[redacted]             GET    200    780b  618ms
https://theomancy.app.telenor.com.pk/api/services-portfolio/portfolio/v2/0340               GET    200    72b   1s
https://theomancy.app.telenor.com.pk/api/customer/usage/history/0340[redacted]              POST   200    1.1kb 316ms
https://firebaselogging-pa.googleapis.com/v1/firelog/legacy/batchlog                        POST   200    1.4kb 2s
https://theomancy.app.telenor.com.pk/api/customer/tax-certificate/verification/0340[redacted] POST 200    194b  1s
https://firebaselogging-pa.googleapis.com/v1/firelog/legacy/batchlog                        POST   200    1006b 2s
https://theomancy.app.telenor.com.pk/api/customer/tax-certificate/download/0340[redacted]   POST   200    305b  341ms
https://firebaselogging-pa.googleapis.com/v1/firelog/legacy/batchlog                        POST   200    1007b 2s
https://mobile.useinsider.com/api/v3/session/stop                                           POST   200    21.2kb 429ms
https://business-api.tiktok.com/open_api/business_sdk_config/get/?disable2Dretention=false&app_ver...GET 200 195b 205ms
https://mobile.useinsider.com/api/v3/session/start                                          POST   200    477b  187ms
https://business-api.tiktok.com/open_api/v1.2/app/monitor/                                  POST   200    2.6kb 115ms
https://theomancy.app.telenor.com.pk/api/offers-campaigns/offers/exclusive/basic/0340[redacted] GET   200    111b  328ms
```

[decoded gzip] JSON

```
{
    "data": {
        "records": [
            {
                "datetime": "20241119095505",
                "fromNum": "92340[redacted]",
                "onNet": "1",
                "smsCharges": "Rs. 0.00",
                "toNum": "9234[redacted]"
            },
            {
                "datetime": "20241119095422",
                "fromNum": "9234[redacted]",
                "onNet": "1",
                "smsCharges": "Rs. 0.00",
                "toNum": "92349[redacted]"
            },
            {
                "datetime": "20241119095352",
                "fromNum": "9234[redacted]",
                "onNet": "1",
                "smsCharges": "Rs. 0.00",
                "toNum": "92349[redacted]"
            },
            {
                "datetime": "20241119095309",
                "fromNum": "9234[redacted]",
                "onNet": "1",
                "smsCharges": "Rs. 0.00",
                "toNum": "9234[redacted]"
            },
            {
                "datetime": "20241119095003",
                "fromNum": "92340[redacted]",
                "onNet": "1",
                "smsCharges": "Rs. 0.00",
```

Figure 28: SMS Records for the My Telenor App [58].



Serial No 00000000000000000004076119 Original / Duplicate
MSISDN 03315096014
Certified that the sum of Rupees **2,360.82**

TWO THOUSAND THREE HUNDRED SIXTY Rupees EIGHTY-TWO Paisas

on account of income tax has been deducted/collected from	[redacted] Username [redacted] Physical Address
having NTN number	
holder of CNIC No.	[redacted]
on	
Or during the period	From MAR-2022 To MAR-2023
Under section	236 of the Income Tax Ordinance, 2001
On account of	telephone services
vide	
on the value/amount of Rupee	15,738.18

This is to further certify that the tax collected/deducted has been deposited in the Federal Government Account as per the following details:

Date of deposit.	SBP/NBP/ Treasury.	Branch/City.	Account (Rupees)	Challan /Treasury No/CPR No.

Company / office etc. collecting/deducting the tax

Name	PAK TELECOM MOBILE LIMITED
Address	[redacted]
NTN	[redacted]
Date	Thursday, 11 July, 2024

Please note that this is a computer generated document and does not require any signature.

Pak Telecom Mobile Limited

Figure 29: Tax Certificate generated by the UPTCL App [71].