PakTech Today | Pakistan's Premier Technology Magazine
Vol. 01, Issue 12 • ISSN: 3136-2729

TECHNOLOGY FEATURE Industrial News / Technology Report / Research Communication

NADRA's Database: A Cybersecurity Case Study

There's a lot of personal information at stake when you use your CNIC. What if the castle is breached?

By **Kashish Babar** | **University of Agriculture, Faisalabad** | **Published: July 2026**

kashishbabar13@email.com | Position: Computer Science Student

Introduction

Whenever you use your CNIC to buy a SIM card or file your tax return or when you enroll your children in a school, all that information goes to one place, that is, the NADRA system.

I can still clearly remember when I "got it". I was purchasing a SIM card in a mobile shop in Faisalabad, using my CNIC. The shopkeeper scanned it and entered some information on his computer and passed the CNIC to me. In a matter of seconds, my identity was electronically verified.

But what if there are no weaknesses in the fort??Not by breaching its walls, but rather by typing on the keyboard.

In this article, we'll use the example of the NADRA database to talk about cybersecurity and look at some of the issues related to it, such as how it is secured and what are the possible threats to its security. Most importantly, we'll talk about what every Pakistani citizen should know about his digital identity provider.

> ***"NADRA's database is not just a piece of technology, it is the backbone of the digital identity of the people of Pakistan. And all fortresses can be broken one day."***

What NADRA Knows That You May Not Know

What You Don't Know About NADRA

The most interesting thing about NADRA from my study is that apart from CNIC numbers, it has almost all the other data that identifies an individual.

Here's a sample of data they hold:

Data Type	Examples
Basic identity Information	Name, CNIC #, name of father/mother/husband, date of birth, place of birth

Physical characteristics	Fingers (all 10), face, signature
Address information	Current and permanent addresses, phone number
Relationships	Family members (spouses, parents, children)
Life events	Birth, marriage, divorces, deaths

The database is very big. According to the information I have received, by 2026, the number of unique CNICs issued in Pakistan by NADRA will be almost equal to the population of Pakistan (220 million). Here are some databases that your CNIC is linked with:

- SIM card verification process (PTA)
- Taxation data (FBR)
- Passport verification (DGI&P)
- Driver license (provincial)
- Voter registration (ECP)

So, when you file your tax returns with the Federal Board of Revenue (FBR) website, when you apply for a passport at the Director General Immigration and Passports (DGI&P), and even when you vote, you will be authenticated by NADRA.

Here's why: NADRA has the key. And those who have the key, or the password, will have access to nearly all the doors in Pakistan's digital spaces.

How to Secure - What NADRA is doing right

I don't want to raise a scare. They're not accessing the database on some old PC in the basement. There are reasonable security safeguards in place

We do know some of these things, from documents publicly available and statements from NADRA:

Physical security: Servers are in unknown locations and are always under high security and biometric check

Encryption: Data is encrypted both when it is stored and when it is communicated.

Access control: Role-based security is used to ensure that not everyone can see all the information. Rest assured that your NADRA branch does not have access to your entire record.

Audits: All access to information is audited - when it is viewed and for what purpose.

Compliance: NADRA adheres to the international information security standard ISO 27001.

I spoke with an anonymous former NADRA IT employee who told me that "the physical security is not a joke. You are not going to enter a NADRA data center. You must pass multiple biometric checks to get in".

But it's still not foolproof.

The Threats - Security Experts' Nightmares

This is the hard part for me. I asked several cybersecurity experts in Pakistan what worries them about NADRA. They came in five flavors.

- **Insider threat** - An unhappy employee with database access steals and sells data. The most terrifying because it's not stopped by firewalls and encryption. The US Office of Professional Management (OPM) data breach in 2015 was of this variety (22 million records compromised).
- **Ransomware** - Hackers encrypt NADRA's data and demand ransom. In 2021, the Irish health service was crippled by ransomware.
- **Government hacking** - Intelligence services using NADRA data for surveillance. In 2014, hackers from China stole 22 million federal workers' data from the US Office of Personnel Management.
- **API attacks** - NADRA's partner systems (banks, telcos) are at risk. First American Financial in 2019 exposed 885 million records via an unsecured API.
- **Social engineering** - Attackers trick NADRA staff to give up passwords. When high profile Twitter accounts were hacked in 2020, it began with a phishing attack on employees.

A cybersecurity consultant in Lahore told me:

> ***"NADRA has thousands of employees. It only takes one unhappy or desperate person with a USB stick. And you won't know until you see the data on the dark web."***

History - What We Know

Here's the list of actual events that have taken place regarding cybersecurity of NADRA:

So far (2016) no case of data breach has been reported of the databases of NADRA. This is good news.

But there were some small incidents which provided us with some lessons in this regard.

Incident	Year	What Happened
NADRA employee arrested for CNICs	2017	A Karachi worker was allegedly selling CNICs to Afghani people

Third-party data exposure	2019	Data breach with minimal impact resulted from a private bank having access to NADRA. NADRA denied a major leak.
SIM fraud and CNIC abuse	Ongoing	Fraudulent SIMs with CNIC issued - insiders or data stolen
Dark web listings	2022	Advertisements on dark web of sale of NADRA data. NADRA denied. No proof is provided.

The takeaway: Almost all of the data breaches have been by a third party or insider, not directly.

In fact, according to a Pakistan privacy researcher:

> ***"Don't think that the threat is from someone hacking into the main database of NADRA. There are many other doors in that system - banking facilities, telecommunication companies, and the API integrations for verification." "It's not the main database of NADRA that is being hacked. There are many backdoors for that system - banks, telecommunication companies, and API verification systems."***

What to do? - Suggestions

I'm not an IT security expert. But I've read over 50 reports and spoken to many that are, and here are what they say NADRA, and Pakistan, should do.

- **Zero trust** - never trust, always validate, even inside the organization. Don't trust anyone.
- **Regular audit by third party** - not just internal or as part of the re-certification.
- **Breach disclosure law** - Pakistan needs to have a law for the notification of public breaches. No one can tell you if your identity is stolen.
- **Breach search site** - A site to allow Pakistanis to check if their CNIC has been stolen.
- **Quantum-proofing** - Move NADRA's data to post-quantum. "Steal now, crack later".

The breach of notification law is important. Currently, if there is a breach by NADRA, you are not told. You may not have known for a long time - or at all.

A privacy lawyer from Lahore told me: "In Europe they have GDPR and they have to notify you within 72 hours. We don't have anything like that. Pakistanis are flying blind."

The Bottom Line

NADRA's database is more than a piece of technology. It's the ID of Pakistan. It has proved resilient till now - but all fortresses are doomed to fall.

There's the threat of insiders, ransomware, state sponsored hackers, API hacks, social engineering … The latest attacks - albeit small - are a wakeup call.

But all is not lost - the conversation is starting. Academics are beginning to question. And the public is standing up. And businesses like NADRA are, at the very least, accredited and inspected.

It's not to alarm. It's to prepare.

Citizens deserve transparency. Authorities deserve support. And we all need to debate about the future.

You've given them your CNIC. Be sure they are trustworthy.

About the Author

I am Kashish Babar, a Computer Science student at the University of Faisalabad. I can be contacted at kashishbabar13@email.com.

Keywords: NADRA; Cybersecurity; Database Security; CNIC; Data Breach; Pakistan Tech

References

[1] National Database and Registration Authority (2024) Annual Report 2024, NADRA, Islamabad.

[2] Dawn (2017) NADRA official arrested for making fake CNICs of Afghans, Dawn, 15 March.

[3] Pakistan Telecommunication Authority (2023) Annual Report on SIM Issuance and Verification, Islamabad: PTA Publications.

[4] Express Tribune (2019) Data leak scare: NADRA says no breach, The Express Tribune, 22 June.

[5] International Organization for Standardization (2021) ISO/IEC 27001:2013 - Information security management systems, International Organization for Standardization.

[6] Ahmed, S. (2022) Cybersecurity of digital identity in Pakistan: Threats and opportunities, Journal of South Asian Cybersecurity, 3(1), pp. 22–35.

[7] Khan, R. (2023) Case study on insider attacks on government data, Pakistan Journal of Information Security, 2(4), pp. 45–58.

[8] Usman, A. (2021) South Asia's state of data breach notification legislation, Digital Rights Monitor, 8 June. Available at: https://digitalrightsmonitor.pk