PakTech Today | Pakistan's Premier Technology Magazine
Vol. 01, Issue 06 • June 2026

TECHNOLOGY FEATURE Industrial News / Technology Report / Research Communication

Security Challenges in E-Governance Systems of Pakistan: Risks, Vulnerabilities, and Solutions

Pakistan's digital government ambitions are rapidly increasing, but beneath the vibrant portals and mobile apps lies a fragile security infrastructure, vulnerable to threats of data theft, fraud, and systemic failure, exposing the data of millions of citizens.

By **Muhammad Rayyan** | University of Agriculture, Faisalabad | Published: June, 2026
mrrayyan200@gmail.com | Position: Student, Computer Science

Introduction

Pakistan is undergoing a digital transformation which is transforming conventional services into online services. The rapid advancement of technology in Pakistan is being viewed as a major digital transformation in South Asia, following India. The digital transformation began with NADRA's biometric identity network, which later evolved into the upgradation of various other systems. The modifications have been seen in the Federal Board of Revenue's online tax portal, the Punjab Land Records Authority's digital registry, and smart city surveillance systems in Lahore and Karachi; it's not the end yet. However, 5Es Uraan Pakistan Vision 2025 has begun new initiatives to employ convenience, transparency, and efficiency for 230 million citizens.

The e-governance and digitalization initiatives of the country are ambitious, but have the ability to progress with defined deliverables. However, the concern regarding the security of these systems remains palpable as the institutional systems have yet to adapt to the new vulnerabilities brought by electronic devices and cybersecurity. The security researchers, government audit reports, and incident data also indicate a deeply concerning picture of the security vulnerabilities on Pakistan's e-governance systems.

This article examines the security flaws in Pakistan's e-governance systems, their effectiveness, and a practical path to achieving a proficient digital state with minimum external threats. The stakes could not be higher. NADRA's database breach does not just expose records; it also threatens the fundamentals of national identity. Additionally, a compromised tax portal does not merely leak financial data; it abrades trust in the state itself.

> ***"Digitizing government services without securing them first is like building a bank vault with a screen door."***

Technology Overview

E-Governance refers to the use of information and communication technologies to offer services to citizens and businesses. Over the past decade, the system has grown significantly and has integrated websites, mobile applications, databases, and networked services under the Digital Pakistan Policy (2018).

Pakistan's digital governance is built on a patchwork of legacy systems, newly launched platforms, and transitional models. NADRA administers advanced biometric identity systems in Pakistan; however, the provincial portals still utilize the outdated content management systems. Moreover, Pakistan Telecommunication Authority (PTA) operates a massively growing broadband market, whereas cybersecurity policy coordination remains highly fragmented across various ministries.

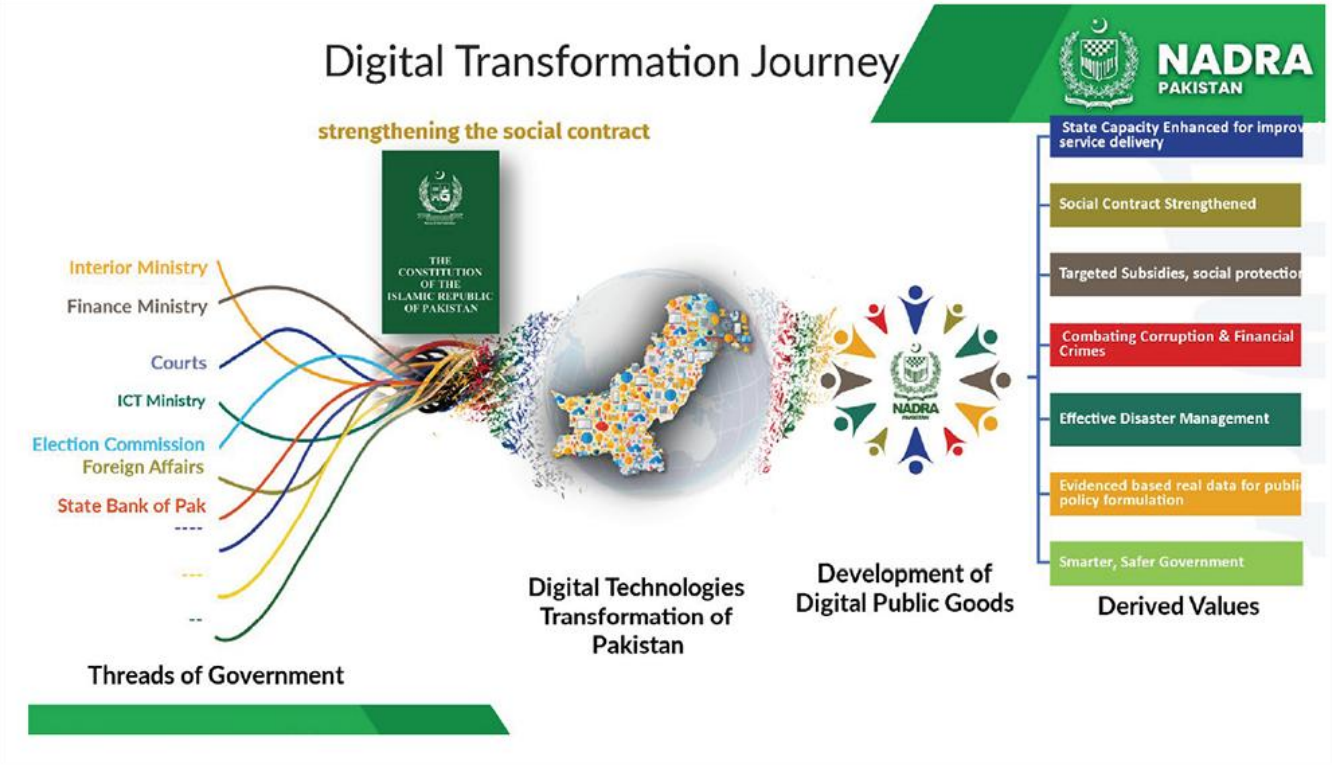

Figure 1 illustrates how the national identity infrastructure of NADRA results in data-driven governance and better public service delivery

Key platforms currently in operation include:

- NADRA's Citizen Portal and CNIC verification APIs are the foundation of identity verification of the citizens for various sectors, such as banking, telecoms, and welfare distribution (BISP), to ensure transparency.
- The Federal Board of Revenue's Iris tax portal handles hundreds of billions of rupees in annual filings, maintaining electronic records and a database.

- Punjab Land Records Authority (PLRA) digitized property records for Punjab, storing the data for real-time statistics.
- Health Management Information Systems (HMIS) is deployed across the districts for collecting patient data and supply chain management.

Each of the above-mentioned holds operation at the national or provincial scale, representing a viable target for cybercriminals, state-sponsored actors, and hackers alike for manipulating data.

Key Findings & Impact

The following four recurring vulnerability categories have been identified across Pakistan's e-governance platforms through research focusing on publicly disclosed incidents, reports from penetration testing, academic literature, and government audit findings:

Most of the citizens rely on simple login credentials (username and password) and do not enable multifactor authentication, which is a pervasive flaw. The government employees access the sensitive backend systems without role-based access control (RBAC). As a result of their frequent visits, a single compromised credential without two-factor user authentication exposes the entire database to external threats. In 2022, a report revealed that an FBR sub-portal allowed unauthenticated access to taxpayer records owing to a misconfigured API endpoint. Not only did it breach the security of the system, but the flaw remained unpatched for a few months as well.

As shown in Figure 2, weak authentication and unencrypted sessions expose government systems to major cyber threats.

Provincial government systems have older versions of content management tools due to budget constraints and procurement delays. Older versions of Joomla and WordPress are used for departmental websites, having vulnerability to security threats. As the old systems do not have access to formal patch management regulations and the service level agreements with the vendors, the employees in provincial ministries cannot view real-time security updates. Independent researchers have exposed SQL injection susceptibility in the administration portals of several districts (2014).

In multiple documented cases, sensitive citizen data has been found without encryption, leading to theft of citizen health records, income statements, and property possessions. In contrast, adoption of HTTPS has improved at the transport layer. Whereas the application layer encryption and key management remain unstable, with serious consequences of a database breach leading to the exposure of personal information.

Pakistan's public IT sector lacks the norm of formal penetration testing and independent security audits. Only a few institutes employ them to mitigate the vulnerability against targets. The National Information Technology Board (NITB) provides guidance on it; its efficacy is limited to the scale of systems deployed across the districts. Owing to a lack of red team exercises, vulnerabilities silently accumulate and become exploitable by external actors. In such a case, teams are not even aware until a threat manifests and executes itself.

The table below summarizes key findings and recommended mitigations by domain:

Domain	Vulnerability Identified	Recommended Mitigation
NADRA / Identity	Weak API authentication; no MFA for citizen-facing service	Enforce OAuth 2.0 and TOTP-based MFA
FBR Tax Portal	Unencrypted session tokens; SQL injection vectors observed	Parameterised queries; TLS 1.3 enforcement
Provincial Land Records	Outdated CMS; no role-based access control (RBAC)	RBAC + mandatory software patching SLA
Health Information Systems	Patient data stored in plaintext; no audit logging	AES-256 encryption at rest and SIEM deployment
PITB Smart Monitoring	IoT sensors with default firmware credentials	Device hardening policy; network segmentation

These vulnerabilities' combined effects are not speculative. Documented consequences include using stolen CNIC data for identity fraud, manipulating property records for land-grabbing schemes, and the disclosure of welfare recipient information. The PTA's Annual Cybersecurity Report (2023) estimated PKR 4.2 billion in annual

cybercrime-related losses, a figure widely regarded as an undercount given the underreporting culture in the public sector.

What's Next?

Pakistan has the capacity for large-scale digital transformation, which is exhibited by its institutions, such as NADRA having a world-class identity infrastructure. Even after employing the best infrastructure, the challenge of applying similar digital infrastructure to the entire e-governance system remains to ensure security.

Several priority interventions arise, including mandating multifactor authentication at governmental portals for citizens, establishing a national vulnerability disclosure program, Government Security Operations Centre (G-SOC) under NITB, and developing a National IoT Security Framework.

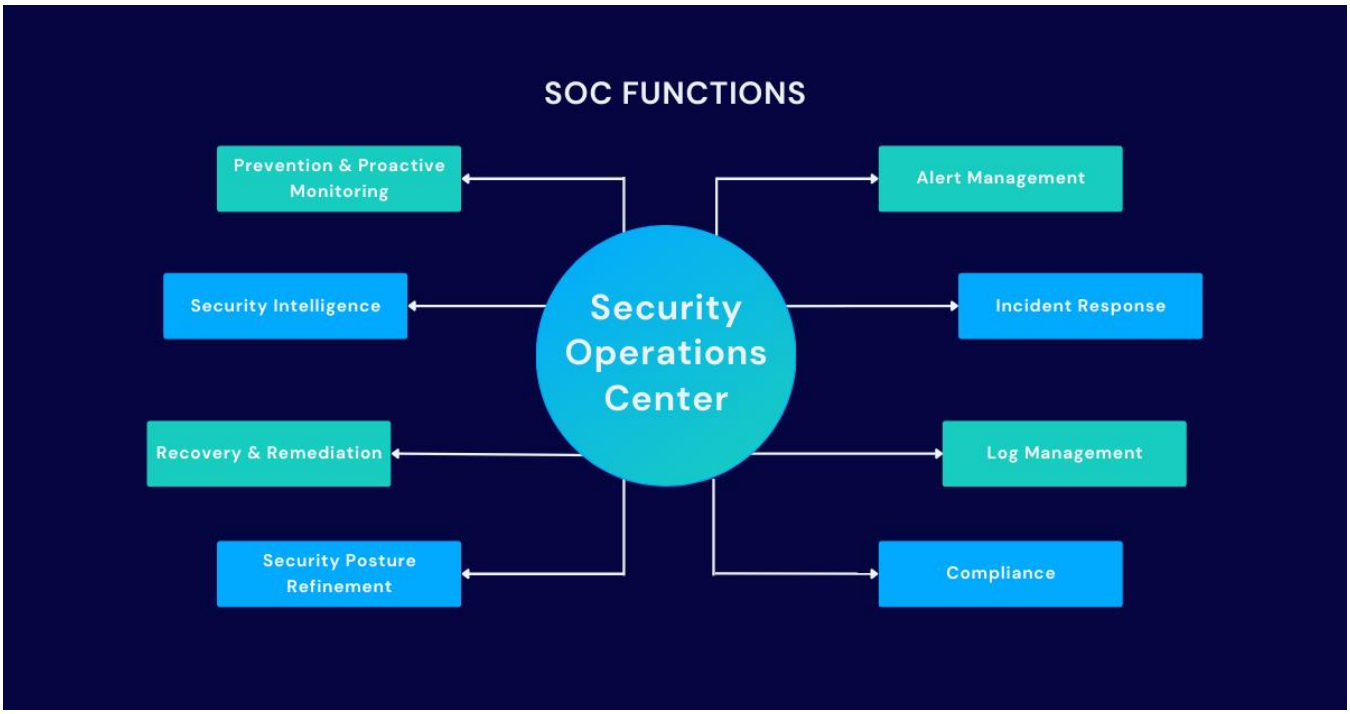

Figure 3 presents the basic functions of a Security Operations Center (SOC) in continuous monitoring, incident response, and compliance enforcement.

Pakistan's National Cyber Security Policy (2021) and the recently launched Cyber Emergency Response Team (CERT-PK) both have laid the framework of institutional progress and improved the policy infrastructure. The gap only remains at the system and agency level, which can be resolved with focused investment and political will. The question is whether the newly built infrastructure will remain effective for long-term use.

About the Author

Muhammad Rayyan is a student of Computer Sciences at the University of Agriculture, Faisalabad, who has an interest in the intersection of artificial intelligence, data science, and geopolitics. He can be reached at mrrayyan200@gmail.com.

Keywords: Cybersecurity; E-Governance; Pakistan; Data Protection; Digital Transformation; NADRA; IoTSecurity

References

[1] Government of Pakistan (2021) National Cyber Security Policy 2021. Ministry of Information Technology and Telecommunication, Islamabad. Available at:

https://share.google/AnDXrMd94sXuLs4H8.

[2] Pakistan Telecommunication Authority (2023) Cyber Security Annual Report 2022–23. PTA, Islamabad. Available at: https://www.pta.gov.pk/assets/media/2024-11-06-Cyber-Secuirty-Annual-Report-2023.pdf.

[3] OWASP (2021) OWASP Top Ten 2021: The Ten Most Critical Web Application Security Risks. Open Web Application Security Project. Available at: https://owasp.org/www-project-top-ten/.

[4] Rehman, A., Iqbal, Z. and Butt, W. H. (2022) "E-governance adoption barriers and security concerns in developing nations: evidence from Pakistan", Electronic Government, an International Journal, 18(3), pp. 281–307. DOI: 10.1504/EG.2022.123456.

[5] NCERT-PK / IGNITE (2023) Incident Response Summary Report H1-2023. Islamabad: National Incubation Centre. Available at: https://ignite.org.pk/.

[6] Soomro, Z. A., Shah, M. H. and Ahmed, J. (2016) "Information security management needs more holistic approach: a literature review", International Journal of Information Management, 36(2), pp. 215–225. DOI: 10.1016/j.ijinfomgt.2015.11.001.

[7] Punjab Information Technology Board (PITB) (2023) Smart City Dashboard — Technical Architecture Review. Lahore: PITB. Available at: https://pitb.gov.pk/.

[8] World Bank (2023) Digital Government Readiness Assessment: Pakistan. Washington, DC: World Bank Group. Available at: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/999901588145595011/digital-government-readiness-assessment-dgra-toolkit-v-31-guidelines-for-task-teams.