THE ASIAN BULLETIN OF BIG DATA MANAGMENT
Vol. 6. Issue 1 (2026)
https://doi.org/10.62019/p3pfmt40

Escalating Cyber Threats: Analyzing Trends, Risks, and Countermeasures in Critical Sectors

Muhammad Imran Ghafoor*, Muhammad Sohaib Roomi, Mehmood Baryalai, Zubair Zaland, Iqra Tabassum, Aliza Sohail

Chronicle

Article history
Received: Feb 12, 2026
Received in the **revised format:** Feb 28, 2026
Accepted: March 15, 2026
Available online: March 30 2026

Muhammad Imran Ghafoor* & Muhammad Sohaib Roomi are currently affiliated with Department of Engineering and Technology Superior University Lahore, Pakistan, Pakistan.
Email: sohaib4039@gmail.com
Email: engr.imranbhatti09@gmail.com

Mehmood Baryalai is currently affiliated with the Dept. of Information Technology, FICT, BUITEMS, Airport Road, Quetta, Pakistan.
Email: mehmood.baryalai@buitms.edu.pk

Zubair Zaland is currently affiliated with the Dept. of Software Engineering FICT, BUITEMS, Airport Road, Quetta, Pakistan.
Email: Zubair.Zaland@buitms.edu.pk

Iqra Tabassum is currently affiliated with the Dept. of Computer Science FICT, BUITEMS, Airport Road, Quetta, Pakistan.
Email: iqra_tabassum47@yahoo.com

Aliza Sohail is currently affiliated with the Dept. of Computer Engineering FICT, BUITEMS, Airport Road, Quetta, Pakistan.
Email: alizasohail232@gmail.com

Corresponding Author*

Abstract

During the period between 2021 and 2026, the situation regarding cyber-attacks against the government bodies, banking platforms, telecom networks, and identity related systems steadily escalated in Pakistan. This paper examines 239 reported cases during the same time and establishes an increment in the frequency of attacks by 294.4 percent between 2021 and 2025. Data breaches that comprise 32.6 percent of all incidents and accumulated privacy exposure of about 744.6 million compromised records shows that the evidence gathered is comprehensive. To go beyond description, the research uses a Privacy Risk Score (PRS) tool in six types of attacks, namely, data breaches, ransomware, phishing and social engineering, distributed denial-of-service attack, website defacement, and advanced persistent threat. The review of the literature provides the basis of the analysis upon Pakistani legal, governance, and technical setting, whereas the experimental section examines the framework of a layered countermeasure structure guided by anonymization, adaptive privacy protection, AI-facilitated detection, and embedding of IoT security. The simulated PRS comparison indicates that privacy risk has been decreased by 84.2 percent when the suggested controls bring down the aggregate Privacy Exposure Index by 92.88 to 14.64. This paper thus provides a policy-relevant and data-supported framework of comprehension on cyber-attacks in Pakistan and its connection of sectoral exposure to the actual countermeasures.

Keywords: cyber-attacks, Pakistan, privacy impact, data breaches, countermeasures, privacy risk score, critical infrastructure security

INTRODUCTION

The cyber risk landscape in Pakistan has reached the point of intersecting with the national security, digital governance, financial stability and the privacy rights. Recent research related to Pakistan talks about cyberterrorism, strategic information warfare, smart-city security, FinTech exposure, adoption of IoT, and the legal challenge of personal data protection in the growing digital systems [1–7]. In other literature, the problem is related to state capacity, counter-terrorism planning, video-security risk, and general trends of cyber interaction [8– 10]. The general impression is obvious: the digital growth of Pakistan is associated with real outcomes, yet it has also significantly increased the attack surface of the participants focusing on the system of state institutions, the commercial platform, and personal information of the citizens.

Particularly, the privacy aspect of this issue is important. The information stolen in Pakistan can include identity records, financial documents, call detail records, biometric contents and other personal identifiable information. But the institutional environment and law is still unequal. Literature also identifies disjointed governance, lax enforcement, and lack of a developed culture of breach notification [11–15]. This implies that cyber incidents are technical as well as accountability, regulatory readiness, and privacy protection failures.

The majority of the literature only provides an overview of the cyber threat environment in Pakistan, or addresses a particular attacker or specific legal issue, or technical protection strategies against them [1, 11, 16–19]. A less common one, however, is a single study, which incorporates evidence of multi-year incidents, privacy-oriented measurement, and an assessment of a countermeasure within a unified framework. The given paper fills that gap with the analysis of the gathered incident list between 2021 and early 2026, the interpretation of privacy implications of such a list, and the experiment with a structured Privacy Risk Score model and a range of six attack types. The paper makes three contributions. First, it presents a consolidated view of attack growth, attack composition, sectoral exposure, and compromised personal-data categories in Pakistan over a multi-year period. Second, it adapts the PRS framework to quantify privacy risk before and after applying a layered countermeasure strategy. Third, it anchors the experimental section in a literature review that connects Pakistan-specific governance weaknesses with current technical remedies, including scalable anonymization, AI-driven monitoring, adaptive differential privacy, and IoT intrusion detection [17, 18, 20–22].

LITERATURE REVIEW

Pakistan's Threat Landscape

The Pakistan-facing literature consistently treats cyber risk as both a security problem and a governance problem. Strategic and legal-national-security studies emphasize cyberterrorism, geopolitical information confrontation, and the burden placed on institutions that are still building coordinated cyber capacity [1–3, 5, 8]. Sectoral and technology-focused work broadens that picture by showing how smart-grid systems, smart-city deployments, digital finance platforms, video-security infrastructures, and IoT-linked services enlarge the attack surface [4, 6, 7, 9, 23–26]. Across these studies, the recurring message is that Pakistan faces a widening cyber threat environment but still lacks a uniformly audited public reporting structure for incident measurement [1, 10, 16].

Privacy, Law, and Governance Gaps

The privacy literature shows a recurring tension between expanding digital monitoring and incomplete legal protection. Butt et al. argue that Article 14 provides only an indirect and underdeveloped privacy foundation for the digital age [12]. Masudi and Mustafa similarly describe the legal framework as fragmented, enforcement-limited, and dependent on overlapping statutes rather than a coherent data-protection architecture [11]. Aziz et al. show that privacy remains less fully developed than security in Pakistan's cyber discourse [14], while Bentotahewa et al. show that GDPR-style compliance challenges in South Asia are structural rather than incidental [15]. Related victimization and human-factor studies reinforce the same point by showing how cyber-victimization, social engineering, and the broader rights discourse all deepen the privacy consequences of technical compromise [13, 27, 28]. Together,

these works explain why cyber-attacks in Pakistan produce not only operational disruption but also long-lasting privacy harm.

Technical Countermeasures in Recent Research

Recent technical literature points to a set of remedies that are particularly relevant for Pakistan. The privacy-preserving line begins with early Map Reduce-based platform and anonymized-classification studies and then develops into scalable anonymization approaches for distributed environments [20, 29–35]. Related studies extend this line through adaptive differential privacy and privacy-aware sensing frameworks [21, 36]. In parallel, IoT and network security research highlights the importance of continuous monitoring, intrusion detection, phishing detection, smart-home privacy protection, and big-data-assisted security analytics [18, 19, 22, 37–41]. AI-focused surveys reinforce the same point by showing how anomaly detection, automated response, adversarial evaluation, and ensemble methods can increase detection speed in resource-constrained environments [17, 42–49].

Supporting Analytical and Experimental Foundations

Beyond directly security-focused studies, a wider set of analytical papers strengthens the methodological base for the experimental sections of this paper. Platform-performance studies, password-security design work, display-classification experiments, and ownership verification research help frame the problem of handling high-volume digital records, securing access, and preserving trust in distributed environments [50–53]. A second group of studies contributes transferable modeling techniques for noisy, high-dimensional, and multimodal data streams, including spatiotemporal forecasting, convolutional feature extraction, deep sequence models, language and sentiment classification, and image-restoration pipelines [54–72]. These studies are not all cyber-attack papers in the narrow sense, but they provide the modeling, classification, and systems foundations that make large-scale cyber experimentation and privacy-impact estimation more technically credible.

Gap Addressed by This Study

Taken together, the existing literature explains why Pakistan faces serious cyber risk and why the privacy consequences can be severe. It also supplies a credible menu of countermeasures. What remains less developed is the link between multi-year incident evidence and privacy focused experimental evaluation. This study addresses that gap by combining a multi-source incident record with a PRS model and then connecting the resulting findings back to the legal and technical literature.

METHODOLOGY

Data Sources and Collection

The study uses a compiled incident record covering January 2021 to March 2026. Incidents were assembled from public advisories, institutional disclosures, sector reports, open-source threat intelligence, and verified reporting on cyber events affecting Pakistani targets. Each record includes the year, attack type, target sector, estimated records exposed, and the dominant category of personal data affected. The resulting dataset contains 239 documented incidents across six major attack categories and five main sectors: government, banking and finance, telecom, healthcare, and citizen identity systems.

Privacy Risk Score Framework

To quantify privacy impact, the study uses a Privacy Risk Score defined as:

$$PRS = \frac{P_{attack} \times V_{exploit} \times I_{records}}{C_{mitigation}}$$

Here, P_{attack} captures the baseline probability of a given attack class, $V_{exploit}$ captures exploit severity, $I_{records}$ reflects the logarithmic exposure of compromised records, and $C_{mitigation}$ represents the effectiveness of deployed countermeasures. The attack categories evaluated in the model are data breach, ransomware, phishing and social engineering, DDoS, advanced persistent threat, and website defacement.

To summarize system-wide privacy exposure, the study uses the Privacy Exposure Index:

$$PEI = \sum_{i=1}^{n} w_i \times PRS_i$$

where w_i is the weight assigned to each attack category. The countermeasure coefficients are informed by recent literature on scalable anonymization, adaptive privacy protection, AI-enabled security, and IoT hardening [17, 19–22].

Analysis Setup

The analytical workflow combines descriptive statistics, cross-tabulation, sectoral aggregation, privacy-impact profiling, and PRS-based scenario evaluation. Descriptive analysis is used to identify attack growth, attack composition, and sectoral concentration. Privacy impact analysis aggregates compromised-record exposure across data types. The experimental component then evaluates how the proposed countermeasure framework changes PRS values by category and reduces aggregate privacy exposure.

Experimental Support from Prior Modeling Work

The experimental design is also supported by prior work on predictive modeling, feature fusion, and large-scale data handling. Studies on distributed processing performance, featurerich classification, adversarial robustness, GAN-based anomaly analysis, and applied deep learning suggest that hybrid pipelines are often more useful than single-technique systems when the data are heterogeneous and partially observed [42, 43, 46, 50, 64]. In the context of cyber experimentation, this justifies combining frequency-based exposure estimation with mitigation coefficients rather than relying on a single static severity rule. Similarly, work on phishing classification, intrusion detection, IoT security, and adaptive privacy protection supports the choice to model countermeasures as layered controls that act differently across attack categories [18, 19, 21, 37–39]. More broadly, studies on forecasting, sequence learning, multilingual analysis, and image-based deep learning show why resilient cyber analytics increasingly depend on flexible model families that can ingest different evidence types without assuming perfectly clean data [60–62, 65–67].

DATA ANALYSIS AND RESULTS

Attack Growth and Composition

The compiled record shows 239 documented incidents against Pakistani targets between 2021 and March 2026. Incident volume rises from 18 in 2021 to 71 in 2025, which corresponds to a 294.4% increase over that interval. The first quarter of 2026 already contains 22 incidents, indicating that the trend remains elevated rather than stabilized.

Table 1 shows the year-by-type distribution. Data breaches dominate the period with 78 incidents, followed by phishing and social engineering with 59 incidents and ransomware with 40 incidents. Website defacement accounts for 28 incidents, while DDoS and advanced persistent threats each account for 17 incidents. In percentage terms, data breaches represent 32.6% of all incidents, phishing and social engineering 24.7%, ransomware 16.7%, website defacement 11.7%, and both DDoS and APT activity 7.1% each.

Sectoral Exposure and Privacy Impact

Sectoral concentration is also pronounced. Government entities account for 70 incidents, or 29.3% of the total, followed by banking and finance with 64 incidents, or 26.8%. Telecom accounts for 50 incidents, citizen identity systems for 37 incidents, and healthcare for 18 incidents. In aggregate, the incident record contains approximately 744.6 million compromised records. By attack class, data breaches account for the largest share of exposed records at 598.8 million, followed by APT activity at 65.9 million and ransomware at 58.2 million.

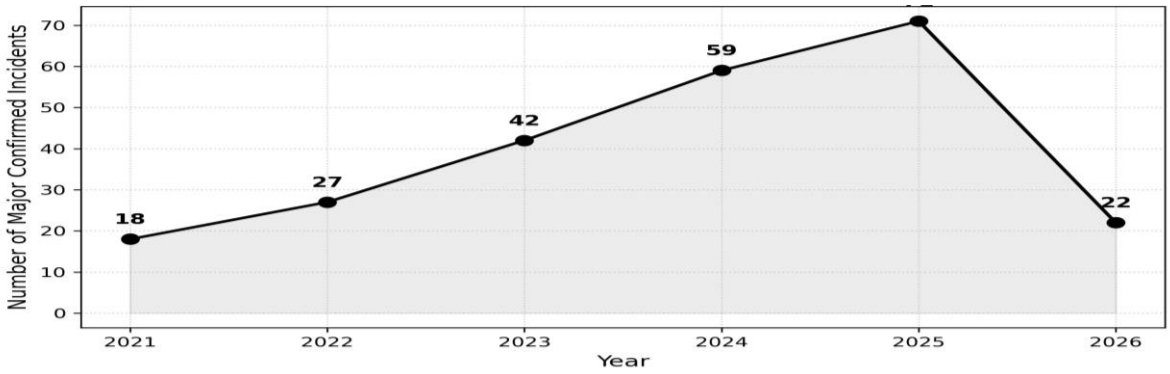

Figure 1. Cyber-attack frequency in Pakistan from 2021 to 2026.

Table 1. Cyber incident distribution by year and attack type.

Year	Data Breach	Ransom ware	Phishing/Social Engineering	DDoS	Website Defacement	APT/Espi onage	Total
2021	7	2	4	1	2	2	18
2022	8	4	8	2	3	2	27
2023	9	6	10	3	8	6	42
2024	17	10	16	5	7	4	59
2025	29	14	15	5	5	3	71
2026*	8	4	6	1	3	0	22
Total	78	40	59	17	28	17	239

*2026 includes January to March only.

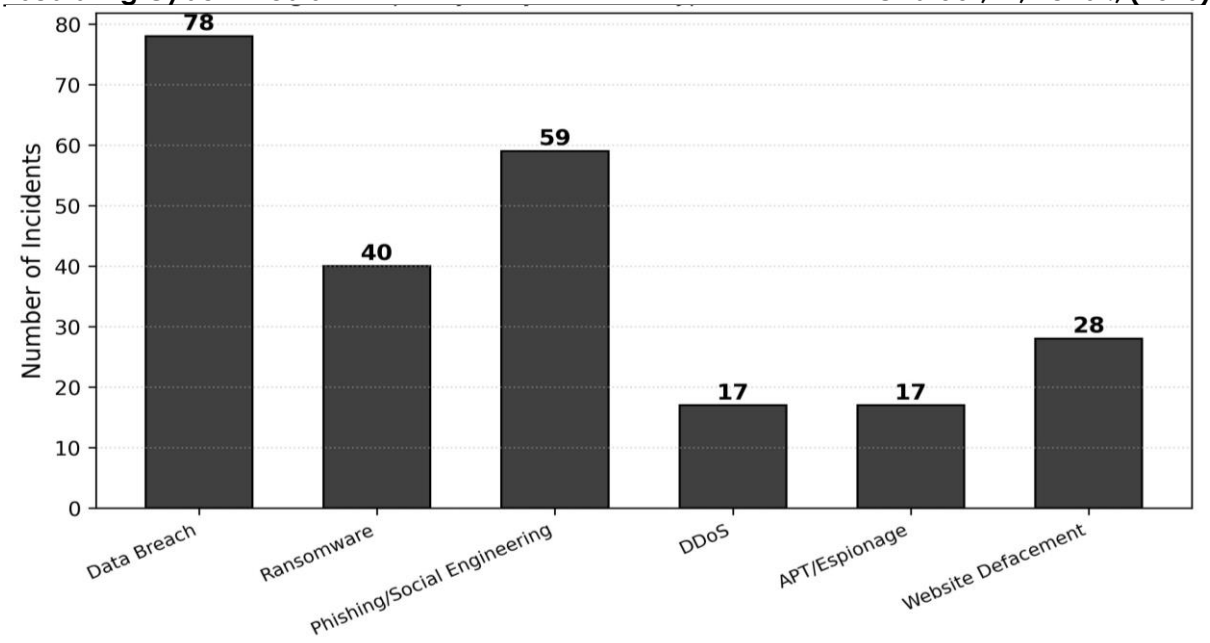

Figure 2. Incident count by attack category.

The privacy impact is concentrated in identity and financial data. CNIC-related data accounts for 230.1 million exposed records, or 30.9% of the total. Financial credentials account for 193.4 million records, or 26.0%, while call detail records account for 188.6 million, or 25.3%. Biometric data and other forms of personally identifiable information make up the remaining share. These results show that privacy harm in Pakistan is not limited to abstract confidentiality loss; it involves the compromise of identity, financial, and communications data at scale.

Privacy Risk Score Evaluation

The experimental component evaluates a layered countermeasure framework that combines encryption, scalable anonymization, adaptive differential privacy, AI-enabled detection, intrusion monitoring, IoT hardening, and organizational controls. Table 2 reports the PRS values before and after applying the mitigation coefficients. Data breach risk remains the highest baseline category, followed by ransomware and phishing/social engineering. After countermeasures are applied, the aggregate Privacy Exposure Index falls from 92.88 to 14.64, corresponding to an 84.2% reduction in modeled privacy exposure.

The category-level reductions are strongest where the framework combines preventive controls with privacy-preserving data handling. For data breaches, scalable anonymization and encryption reduce the long-term value of stolen records [20, 34]. For phishing and social engineering, user-focused controls combine with phishing-detection and anomaly-analysis systems to reduce both attack probability and exploit success [17, 38, 39]. For APT and IoT-related exposure, network hardening, smart-environment privacy protection, routing efficiency, and intrusion detection remain critical [18, 19, 22, 37, 40, 41].

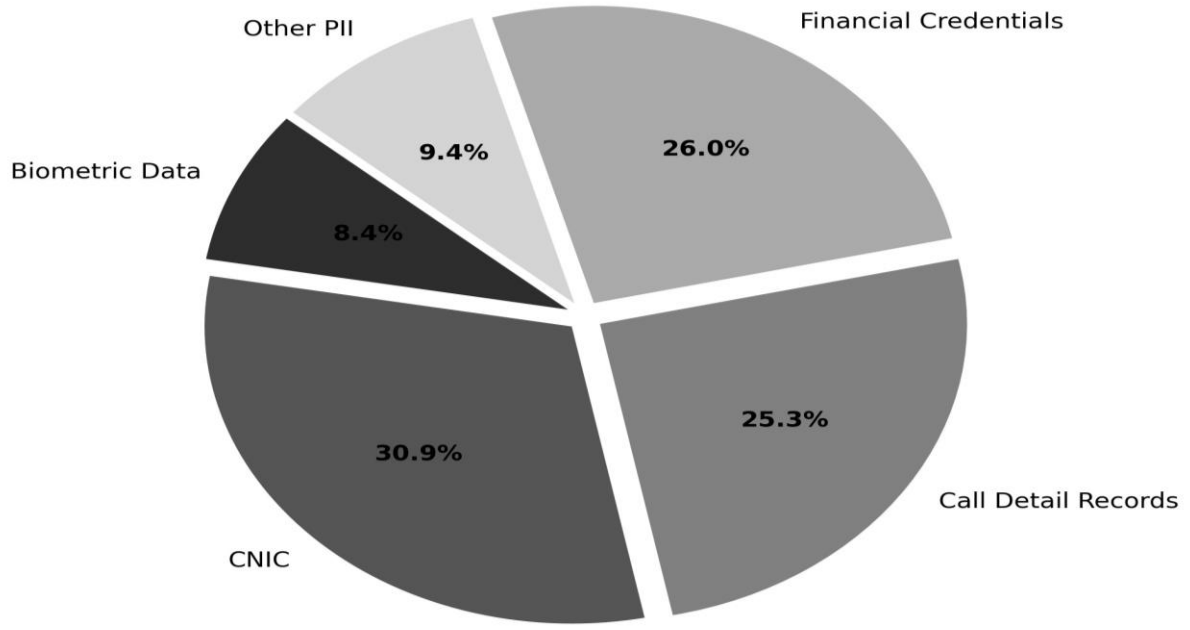

Figure 3. Distribution of privacy impact by compromised data type.

Table 2. Privacy Risk Score before and after countermeasures.

Category	P_{attack}	$V_{exploit}$	$I_{records}$	PRS Before	PRS After	Reduction
Data Breach	0.30	7.50	6.89	154.92	23.83	84.6%
Ransomware	0.18	8.20	6.16	90.96	12.99	85.7%
Phishing/Social Engineering	0.24	6.80	5.49	89.63	16.30	81.8%
DDoS	0.10	5.50	4.84	26.62	3.33	87.5%
APT/Espionage	0.08	9.00	6.59	47.44	7.91	83.3%
Website Defacement	0.10	4.20	4.90	20.59	2.75	86.7%
Aggregate PEI	—	—	—	92.88	14.64	84.2%

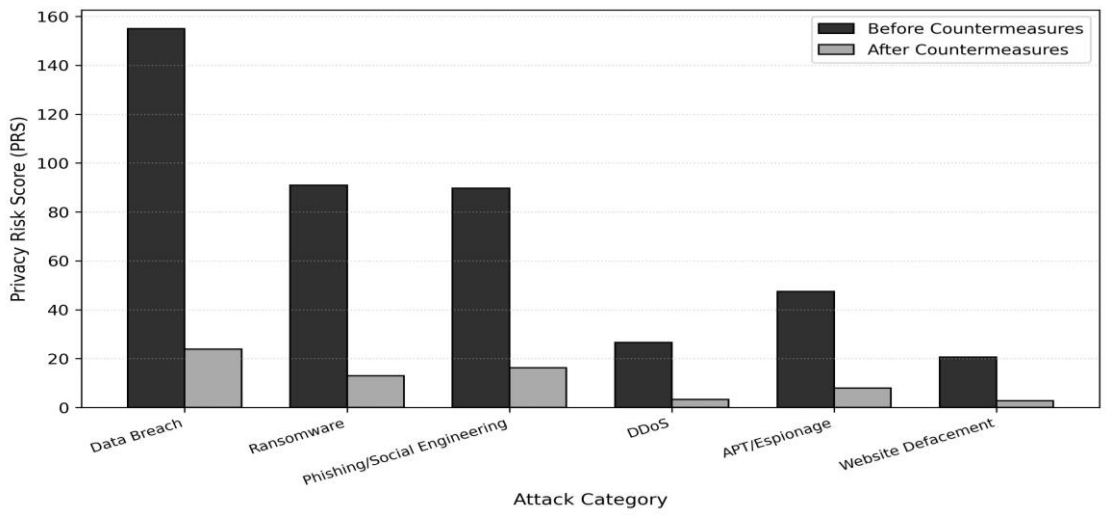

Figure 4. Privacy Risk Score comparison before and after countermeasures.

The broader cyberterrorism and governance literature also matters here because sustained threat pressure changes the design requirements for defenses and public-sector preparedness [1, 8, 73].

DISCUSSION

The results show that cyber-attacks in Pakistan are not distributed randomly. Government, banking, telecom, and identity-related systems absorb most of the documented pressure because they hold the most valuable combinations of personal, financial, and communications data. The scale of compromised records further suggests that privacy exposure in Pakistan should be treated as a national governance issue rather than only as a technical-security problem.

The PRS experiment reinforces the importance of layered countermeasures. The strongest reductions occur when privacy-preserving data handling is combined with detection, response, and governance controls rather than treated as a standalone fix. This is consistent with the recent literature, which increasingly connects scalable anonymization, adaptive privacy protection, AI-assisted detection, multilingual or multimodal analytics, and IoT security monitoring as complementary rather than isolated interventions [17, 19–21, 62, 63, 65]. The same conclusion is supported by recent application-driven deep learning studies that show hybrid models are often most effective when the evidence is noisy, distributed, and operationally constrained [49, 68–72].

Several limitations remain. The incident record is compiled from available reporting and therefore is likely to understate true attack volume, especially in sectors where disclosure remains weak. The PRS experiment is model-based and depends on selected coefficients for exploit severity and mitigation effectiveness. Even so, the combined descriptive and experimental findings provide a more structured basis for discussion than incident description alone.

CONCLUSION AND FUTURE WORK

This paper examined 239 documented cyber incidents affecting Pakistan between 2021 and early 2026 and showed a sharp increase in attack activity over the period. Data breaches, phishing and social engineering, and ransomware emerge as the most consequential categories by frequency and privacy impact, while government and financial systems remain the most exposed sectors. The overall record points to a large and sustained burden on identity, financial, and communications data.

The PRS framework extends the study beyond description by showing how a layered countermeasure strategy can reduce modeled privacy exposure substantially. The results support a practical conclusion: Pakistan's cyber-defense agenda should prioritize breach resilience, privacy-preserving data handling, stronger incident detection, and sector-specific governance measures rather than relying on any single technical control.

Future work should extend this framework with continuously updated incident feeds, deeper validation against institution-level outcomes, and comparative analysis across South Asian settings. Additional work on breach-notification practice, public-sector cyber capacity, and measured deployment of privacy-preserving analytics would also strengthen the link between research findings and operational policy.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the contributors to the research and their different affiliations.
Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.
Availability of data and material: In the approach, the data sources for the variables are stated.
Authors' contributions: Each author participated equally in the creation of this work.
Conflicts of Interest: The authors declare no conflict of interest.
Consent to Participate: Yes
Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

A. Asghar, A. Shifa, and M. N. Asghar, "Survey on video security: Examining threats, challenges, and future trends." *Computers, Materials & Continua*, vol. 80, no. 3, 2024. [10] T. Baisley and Y. Cherrat, "Cyber threats and engagements in 2022," 2023, report.

A. Jahangeer, S. U. Bazai, S. Aslam, S. Marjan, M. Anas, and S. H. Hashemi, "A review on the security of iot networks: From network layer's perspective," *IEEE Access*, vol. 11, pp. 71073–71087, 2023.

A. Sabir, S. U. Bazai, M. I. Ghafoor, U. A. Bhatti, A. Umidjon, A. Ashirova, and M. Allaberganova, "Optimizing breast cancer classification accuracy with hybrid deep learning and advanced image processing," in *2025 IEEE 6th International Conference on Computer, Big Data, Artificial Intelligence (ICCBD+ AI)*. IEEE, 2025, pp. 1–5.

A. Saeed, T. U. Rehman, A. Abid, A. Zawar, and S. A. A. Bukhari, "Cyber legislation and cyber-victimization in pakistan," *AL-HAYAT Research Journal*, vol. 2, no. 3, 2025.

A. Topbaş, A. Jamil, A. A. Hameed, S. M. Ali, S. U. Bazai, and S. A. Shah, "Sentiment analysis for covid-19 tweets using recurrent neural network (rnn) and bidirectional encoder representations (bert) models," in *2021 International Conference on Computing, Electronic and Electrical Engineering (ICE Cube)*. IEEE, 2021, pp. 1–6.

B. Ghafoor, S. U. Bazai, A. Badar, A. Umidjon, Y. Bakhrom, R. R. Rakhimov, and U. A. Bhatti, "Plant disease detection using pre-trained deep learning models: A study on low-quality images," in *2025 IEEE 6th International Conference on Computer, Big Data, Artificial Intelligence (ICCBD+ AI)*. IEEE, 2025, pp. 1–6.

G. Ali, M. M. Mijwil, B. A. Buruga, and M. Abotaleb, "A comprehensive review on cybersecurity issues and their mitigation measures in fintech," 2024, review manuscript.

H. Abbas, "Cyber terrorism and the future of pakistan's national security," *Spectrum of Engineering Sciences*, vol. 4, no. 1, pp. 888–907, 2026.

H. Han, S. U. Bazai, M. A. Bhatti, A. Basit, A. Wahid, U. A. Bhatti, Y. Y. Ghadi, and A. Algarni, "Hybrid climate forecasting: Variational mode decomposition and convolutional neural network with long-term short memory." *Polish Journal of Environmental Studies*, vol. 33, no. 2, 2024.

I. Batool, S. U. Bazai, L. Baloch, M. I. Ghafoor *et al.*, "Exploring advanced deep learning methods for enhancing image clarity: A review," in *2024 5th International Conference on Innovative Computing (ICIC)*. IEEE, 2024, pp. 1–8.

I. Nasir, S. U. Bazai, M. I. Ghafoor, and S. Marjan, "Urdu sentiment analysis using deep learning," in *2024 18th International Conference on Open Source Systems and Technologies (ICOSST)*. IEEE, 2024, pp. 1–7.

I. Tabassum and S. U. Bazai, "Augmenting multimedia analysis: A fusion of deep learning with differential privacy," in *Deep Learning for Multimedia Processing Applications*. CRC Press, 2024, pp. 194–215.

I. Tabassum, S. U. Bazai, M. I. Ghafoor, U. A. Bhatti, S. Ullah, and S. Akram, "A context-aware adaptive differential privacy for privacy-aware users in mobile crowd sensing," in *2025 International Conference on Frontiers of Information Technology (FIT)*. IEEE, 2025, pp. 1–6.

I. Tabassum, S. U. Bazai, Z. Zaland, S. Marjan, M. Z. Khan, and M. I. Ghafoor, "Cyber security's silver bullet-a systematic literature review of ai-powered security," in *2022 3rd International Informatics and Software Engineering Conference (IISEC)*. IEEE, 2022, pp. 1–7.

J. A. Masudi and N. Mustafa, "Cyber security and data privacy law in pakistan: Protecting information and privacy in the digital age," *Pakistan Journal of International Affairs*, vol. 6, no. 3, 2023.

J. Joseph, "Cybersecurity vis-à-vis data privacy: An ethico-legal framework for a dignified cyberspace," in *Legal and Ethical Challenges in Data Privacy Rights and Cybersecurity*. IGI Global Scientific Publishing, 2026, pp. 127–154.

K. Hameed, R. Naha, and F. Hameed, "Digital transformation for sustainable health and well-being: a review and future research directions," *Discover Sustainability*, vol. 5, no. 1, p. 104, 2024.

M. A. Shoaib, R. Ali, S. U. Bazai, and T. Mir, "Deep learning techniques for image segmentation and data annotation," in *Modern Intelligent Techniques for Image Processing*. IGI Global Scientific Publishing, 2025, pp. 63–94.

M. Aamir, M. A. Bhatti, S. U. Bazai, S. Marjan, A. M. Mirza, A. Wahid, A. Hasnain, and U. A. Bhatti, "Predicting the environmental change of carbon emission patterns in south asia: a deep learning approach using bilstm," *Atmosphere*, vol. 13, no. 12, p. 2011, 2022.

M. Aamir, S. U. Bazai, U. A. Bhatti, J. Li, and H. Mengxing, "Deep learning based applications for multimedia processing applications: Volume 1 and 2," 2024.

M. Aamir, Z. Li, S. U. Bazai, R. A. Wagan, U. A. Bhatti, M. M. Nizamani, and S. Akram, "Spatiotemporal change of air-quality patterns in hubei province—a pre-to post-covid-19 analysis using path analysis and regression," *Atmosphere*, vol. 12, no. 10, p. 1338, 2021.

M. Afzal, M. S. Ansari, N. Ahmad, M. Shahid, and M. Shoeb, "Cyberfraud, usage intention, and cybersecurity awareness among e-banking users in india: an integrated model approach," *Journal of Financial Services Marketing*, vol. 29, no. 4, pp. 1503–1523, 2024.

M. Ahmed, M. I. Ghafoor, S. U. Bazai, S. Sardor, U. A. Bhatti, and T. Eshchanov, "Hybrid ml approach for robust intrusion detection in iot networks," in *2025 IEEE 2nd International Conference on Deep Learning and Computer Vision (DLCV)*. IEEE, 2025, pp. 1–6.

M. Akram, S. U. Bazai, M. I. Ghafoor, S. Akram, Q. M. Ilyas, A. Mehmood, S. Iqbal, and M. A. Rafique, "Eemlcr: Energy-efficient machine learning-based clustering and routing for wireless sensor networks," *IEEE Access*, 2025.

M. Akram, S. U. Bazai, M. Sulaman, and F. Ullah, "Innovative deep learning image technologies: Applications of deep learning in image processing," in *Modern Intelligent Techniques for Image Processing*. IGI Global Scientific Publishing, 2025, pp. 145–180.

M. F. Butt, H. A. R. Saleem, M. A. I. Hashmi, and N. Bano, "The right to privacy in the age of surveillance: Legal protections in pakistan," *Advance Social Science Archive Journal*, vol. 2, no. 4, pp. 1449–1458, 2024.

M. H. Ferdaus, M. G. Kaosar, F. Alharbi, M. S. Ali, M. M. Islam, and R. Buyya, "The digital face of espionage: Analyzing cyber threats to national security," in *Cyber Espionage and National Security Challenges: Cyber Wargaming for Critical Infrastructures*. Springer, 2026, pp. 11–41.

M. Hakimi, A. W. Fazil, and Z. Matin, "Examining cybersecurity factors affecting the adoption and institutionalization of internet of things technologies in developing countries," *Journal of Advanced Computer Knowledge and Algorithms*, vol. 3, no. 1, pp. 26–36, 2026.

M. Hameed, F. Yang, S. U. Bazai, M. I. Ghafoor, A. Alshehri, I. Khan, S. Ullah, M. Baryalai, F. H. Jaskani, and M. Andualem, "Convolutional autoencoder-based deep learning approach for aerosol emission detection using lidar dataset," *Journal of Sensors*, vol. 2022, no. 1, p. 3690312, 2022.

M. Hamza, S. U. Bazai, M. I. Ghafoor, S. Ullah, S. Akram, and M. S. Khan, "Generative adversarial networks (gans) video framework: A systematic literature review," in *2023 International Conference on Energy, Power, Environment, Control, and Computing (ICEPECC)*. IEEE, 2023, pp. 1–5.

M. I. Ghafoor, M. S. Roomi, M. Aqeel, U. Sadiq, and S. U. Bazai, "Multi-features classification of smd screen in smart cities using randomised machine learning algorithms," in *2021 2nd International Informatics and Software Engineering Conference (IISEC)*. IEEE, 2021, pp. 1–5.

M. Muhammad, S. U. Bazai, S. Ullah, S. A. A. Shah, S. Aslam, A. Amphawan, and T.K. Neo, "A systematic literature review on the role of big data in iot security," *Journal of Telecommunications and the Digital Economy*, vol. 12, no. 1, pp. 39–64, 2024.

M. S. Khan, S. U. Bazai, M. I. Ghafoor, S. Marjan, M. Ameen, and S. A. A. Shah, "Forecasting cryptocurrency prices using a gated recurrent unit neural network," in *2023 International Conference on Energy, Power, Environment, Control, and Computing (ICEPECC)*. IEEE, 2023, pp. 1–6.

M. Shabbir, A. Hussain, and T. Rahim, "Cybersecurity: A growing challenge for pakistan," *Annals of Human and Social Sciences*, vol. 6, no. 1, pp. 219–233, 2025.

M. Sulaman, S. ullah Bazai, M. AKram, and M. A. Khan, "The deep learning based smart navigational stick for blind people," *UMT Artificial Intelligence Review*, vol. 2, no. 2, 2022.

N. Ahmed, A. L. Barczak, S. U. Bazai, T. Susnjak, and M. A. Rashid, "Performance analysis of multi-node hadoop cluster based on large data sets," in *2020 IEEE AsiaPacific Conference on Computer Science and Data Engineering (CSDE)*. IEEE, 2020, pp. 1–6.

N. K. Hania, B. Sibghat Ullah, Z. Zubair, D. Sibghat Ullah, A. Saad, A. Angela, F. Ali, and N. Tse-Kian, "A comparative study of convolutional neural networks and recurrent neural networks for chord recognition," *International Journal of Membrane Science and Technology*, vol. 10, no. 2, pp. 1617–1630, 2023. [Online]. Available: https://doi.org/10.15379/ijmst.v10i2.1837

O. Aziz, M. A. Siraj, and A. Rehman, "Privacy challenges in cyber security against cybercrime in digital forensic: A systematic literature review in pakistan," *Journal of Computing & Biomedical Informatics*, vol. 2, no. 2, 2021.

R. K. Shaikh, R. Anjum, and A. Barkat, "Cyber-security beyond borders: Unraveling cross-jurisdictional legal complexities in cyberspace," *ASSAJ*, vol. 5, no. 01, pp. 334–352, 2026.

R. Noor, A. Wahid, S. U. Bazai, A. Khan, M. Fang, S. MS, U. A. Bhatti, and Y. Y. Ghadi, "Dlgan: Undersampled mri reconstruction using deep learning based generative adversarial network," *Biomedical signal processing and control*, vol. 93, p. 106218, 2024.

R. Ullah, S. U. Bazai, U. Aslam, and S. A. A. Shah, "Utilizing blockchain technology to enhance smart home security and privacy," in *Proceedings of International Conference on Information Technology and Applications: ICITA 2022*. Springer Nature Singapore Singapore, 2023, pp. 491–498.

S. A. Agha, S. U. Bazai, and A. Naushad, "Facial expression and key landmarks detection using deep learning techniques," *International Journal of Pattern Recognition and Artificial Intelligence*, 2026.

S. Akram, S. U. Bazai, and S. Marjan, "Classifying traffic signs using convolutional neural networks based on deep learning models," in *Deep Learning for Multimedia Processing Applications*. CRC Press, 2024, pp. 250–269.

S. Akram, S. U. Bazai, M. I. Ghafoor, S. Marjan, M. Hamza, and S. A. A. Shah, "Systematic literature review: Evaluating effects of adversarial attacks and attack generation methods," in *2023 International Conference on Energy, Power, Environment, Control, and Computing (ICEPECC)*. IEEE, 2023, pp. 1–6.

S. Ashraf, C. Choi, and A. Bilal, "Ctdmf-sc: cybersecurity threat detection and mitigation framework for smart cities: S. ashraf et al." *International Journal of Information Security*, vol. 25, no. 2, p. 54, 2026.

S. Hussain, S. U. Bazaib, S. Qadir, S. Marjan, P. Pervaiz *et al.*, "Sentiment analysis of balochi text using deep learning," *VAWKUM Transactions on Computer Sciences*, vol. 13, no. 1, pp. 190–200, 2025.

S. Iftikhar, "Cyberterrorism as a global threat: A review on repercussions and countermeasures," *PeerJ Computer Science*, vol. 10, p. e1772, 2024.

S. Kausar and A. R. Laghari, "Social engineering attacks in pakistan: Analyzing the weakest link in cyber security," *Journal of Development and Social Sciences*, vol. 6, no. 1, pp. 364–374, 2025.

S. M. Usman, "Pakistan in the crosshairs and the rising stakes of strategic information warfare," *Journal of Research in Social Sciences*, vol. 12, no. 1, pp. 1–23, 2024.

S. Noor, S. U. Bazai, M. I. Ghafoor, S. Marjan, S. Akram, and F. Ali, "Generative adversarial networks for anomaly detection: a systematic literature review," in *2023 4th International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*. IEEE, 2023, pp. 1–6.

S. Noor, S. U. Bazai, S. Tareen, and S. Ullah, "Detecting phishing urls through deep learning models," in *Deep Learning for Multimedia Processing Applications*. CRC Press, 2024, pp. 176–193.

S. Tareen, S. U. Bazai, S. Ullah, R. Ullah, S. Marjan, and M. I. Ghafoor, "Phishing and intrusion attacks: an overview of classification mechanisms," in *2022 3rd International Informatics and Software Engineering Conference (IISEC)*. IEEE, 2022, pp. 1–5.

S. U. Bazai and J. Jang-Jaccard, "Scalable, high-performance, and generalized subtree data anonymization approach for apache spark," *Electronics*, vol. 10, no. 5, p. 589, 2021.

S. U. Bazai and J. Jang-Jaccard, "In-memory data anonymization using scalable and high performance rdd design," *Electronics*, vol. 9, no. 10, p. 1732, 2020.

S. U. Bazai and J. Jang-Jaccard, "Sparkda: Rdd-based high-performance data anonymization technique for spark platform," in *International conference on network and system security*. Springer International Publishing Cham, 2019, pp. 646–662.

S. U. Bazai, "Building privacy-preservation models for distributed processing platforms: a thesis submitted in partial fulfilment of the requirements for the degree of doctor of philosophy (ph. d.) in computer science, massey university, new Zealand," Ph.D. dissertation, Massey University, 2020.

S. U. Bazai, J. Jang-Jaccard, and H. Alavizadeh, "A novel hybrid approach for multidimensional data anonymization for apache spark," *ACM Transactions on Privacy and Security*, vol. 25, no. 1, pp. 1–25, 2021.

S. U. Bazai, J. Jang-Jaccard, and R. Wang, "Anonymizing k-nn classification on mapreduce," in *International conference on mobile networks and management*. Springer International Publishing Cham, 2017, pp. 364–377.

S. U. Bazai, J. Jang-Jaccard, and X. Zhang, "A privacy preserving platform for mapreduce," in *International conference on applications and techniques in information security*. Springer Singapore Singapore, 2017, pp. 88–99.

S. U. Bazai, J. Jang-Jaccard, and X. Zhang, "Scalable big data privacy with mapreduce," in *Encyclopedia of big data technologies*. Springer, Cham, 2019, pp. 1454–1462.

S. U. Bazai, M. I. Ghafoor, M. Aqeel, and M. S. Roomi, "Kernel virtual machine based high performance environment for grid and jungle computing," in *2021 2nd International Informatics and Software Engineering Conference (IISEC)*. IEEE, 2021, pp. 1–6.

S. Ullah, S. U. Bazai, Z. Zaland, M. I. Ghafoor, A. Haider, and L. Hussain, "Ownership verification for digital art using smart contract and blockchain technology," in *2023 17th International Conference on Open Source Systems and Technologies (ICOSST)*. IEEE, 2023, pp. 1–6.

T. Khattak and R. J. Asghar, "Strategic counter measures to terrorism and extremism in pakistan and insights from home land security: A need for the enactment of pakistan's national counter terrorism department," *Inverge Journal of Social Sciences*, vol. 3, no. 1, pp. 61–74, 2024.

T. Mazhar, D. B. Talpur, T. A. Shloul, Y. Y. Ghadi, I. Haq, I. Ullah, K. Ouahada, and H. Hamam, "Analysis of iot security challenges and its solutions using artificial intelligence," *Brain sciences*, vol. 13, no. 4, p. 683, 2023.

T. Mazhar, H. M. Irfan, S. Khan, I. Haq, I. Ullah, M. Iqbal, and H. Hamam, "Analysis of cyber security attacks and its solutions for the smart grid using machine learning and blockchain methods," *Future Internet*, vol. 15, no. 2, p. 83, 2023.

U. A. Bhatti, H. Mengxing, J. Li, S. Bazai, and M. Aamir, "Deep learning for multimedia processing applications," *Signal Process Pattern Recogn*, 2024.

U. A. Bhatti, H. Mengxing, J. Li, S. U. Bazai, and M. Aamir, "Deep learning for multimedia processing applications: Volume two: Signal processing and pattern recognition," 2024.

U. A. Bhatti, M. Huang, H. Neira-Molina, S. Marjan, M. Baryalai, H. Tang, G. Wu, and S. U. Bazai, "Mffcg–multi feature fusion for hyperspectral image classification using graph attention network," *Expert Systems with Applications*, vol. 229, p. 120496, 2023.

U. A. Bhatti, S. U. Bazai, S. Hussain, S. Fakhar, S. Marjan, P. L. Yee *et al.*, "Deep learning-based trees disease recognition and classification using hyperspectral data." *Computers, Materials & Continua*, vol. 77, no. 1, 2023.

V. Bentotahewa, C. Jayasinghe, and M. Siriwardena, "Solutions to gdpr challenges for south asian countries: A systematic literature review," *SN Computer Science*, vol. 3, no. 170, 2022.

V. Mercan, A. Jamil, A. A. Hameed, I. A. Magsi, S. U. Bazai, and S. A. Shah, "Hate speech and offensive language detection from social media," in *2021 International Conference on Computing, Electronic and Electrical Engineering (ICE Cube)*. IEEE, 2021, pp. 1–5.

Z. Zaland, S. U. Bazai, S. Marjan, and M. Ashraf, "Three-tier password security algorithm for online databases," in *2021 2nd International Informatics and Software Engineering Conference (IISEC)*. IEEE, 2021, pp. 1–6.