International Journal of Cloud Computing and Database Management

**E-ISSN:** 2707-5915
**P-ISSN:** 2707-5907
**Impact Factor (RJIF):** 5.4
IJCCDM 2025; 6(2): 93-99
Journal's Website
Received: 10-09-2025
Accepted: 15-10-2025

**Kaushal Kishor Jha**
Department of BCA, IIMT College of Management, Greater Noida, Uttar Pradesh, India

**Corresponding Author:**
**Kaushal Kishor Jha**
Department of BCA, IIMT College of Management, Greater Noida, Uttar Pradesh, India

# A holistic review of cybersecurity and privacy frameworks in digital ecosystem

**Kaushal Kishor Jha**

**DOI:** https://www.doi.org/10.33545/27075907.2025.v6.i2b.113

**Abstract**
The digital landscape of India has undergone massive changes in the last decade. It was actually fueled by Government ventures called Digital India. Smartphones loaded with digital platforms offer tremendous opportunities to handle a wide range of routine tasks, both personal and professional. Now, AI is also becoming an integral part of everyday work. Digital devices perform swift, smooth and easy execution of a diverse range of tasks. But this day-to-day work with smartphones and other digital devices also involves sensitive and personal information, such as the Aadhaar database, banking details, and account credentials. Therefore, it has posed serious threats to cybersecurity, privacy, and ethics in the digital ecosystem. We have comprehensively discussed these aspects in this review paper.

**Keywords:** Cybersecurity, cyberprivacy, digital ecosystem, blockchain, IoT, privacy by design

## Introduction

The evolution of digital technology has shifted from isolated computing to global hyper-connectivity. Globally, this shift was began with Personal Computer (PC) enbak-1 designed by John Blankenbaker in 1970 (Cooper, 2023) [11], followed by creation of World Wide Web in 1989 by Sir Tim Berners-Lee. It was first window of democratized access of information. First handheld mobile phone call was made by Motorola's Martin Cooper on 3 April1973 (Korn, 2023) [11, 20]. A cost-effective smartphone and cellular data became available in 2010 across India, which further converted in revolutionary mode after launching Jio digital services in India, especially in terms of free unlimited 4G data on 5 September 2016. Today, world is navigating into the era of Artificial Intelligence (AI) and Cloud Computing. It facilitates automated complex tasks and reshapes the corporate and industrial sectors.

The digital story in India starts with Aadhaar in 2009. It was the world's largest biometric ID system which served as digital identity to over 1.377 billion Indians as per Unique Identification Authority of India (UIDAI). This became the foundation for allowing for paperless and cashless service delivery e.g., Direct Benefit Transfers (DBT) related financial transactions. As discussed, Reliance Jio is offering free and low-cost data which makes internet accessible to massive population of India and encourages the digital presence of the public (Mukherjee, 2019) [25]. Later, the global benchmark Unified Payments Interface (UPI) was adopted in 2016 which allow instantaneous bank-to-bank transfers via mobile phones (Mishra *et al.*, 2024) [22]. Today it is inevitable that QR codes are ubiquitously used by huge population inside India i.e., from high-end malls to roadside vegetable vendors.

Counterparts of these benefits are associated with various dark side effects such as Cyber threats, privacy and ethical aspects (Michael *et al.*, 2025) [21]. We might need to be aware of spike in ransomware, phishing scams and data breaches like events in government offices to private companies. The cyber attackers are now becoming smarter and unfortunately our defences and general awareness aren't always working against their strategies to target victim. Regularly, many people are trapping in their scams. This could also be seen as national security risk. However, Government has launched National Cyber Security Policy (2013) and Cyber Surakshit Bharat to cope with such scenarios. But we are still struggling to enforce it and we are unable to find enough technologically skilled people to handle these things. Furthermore, privacy issues with government and private apps are to collect large amounts of personal data without consent of user is also emerged as threat to cyberprivacy and cybersecurity. These data are sometimes used for illegal and criminal activities. Moreover, identity theft, financial fraud, blackmail and extortion, data selling, political

discrediting and harassment are considered major illegal and criminal activities (Wang *et al.*, 2024; Mishra and Sinha, 2022) [43]. However, Digital Personal Data Protection Act (DPDPA) 2023 was released to regulate it (Ahmed and Nasir, 2025) [1]. But people are still concerned regarding government surveillance protocols i.e., where their data are stored and what rights they actually have to protect their data. Presently, India is facing ethical AI bias, fake news and biased algorithms that lack transparency (Tripathi *et al.*, 2023) [41]. Henceforth, present review paper is focused on brief holistic review of cybersecurity and privacy frameworks in the digital ecosystem especially in context of India. Baqer (2024) and Ghadi *et al.* (2023) [8, 17] reported that Federated Learning (FL) is potential solution for smart devices, as it enables smart devices to utilize AI along with data privacy benefits and conserves internet bandwidth. Dritsas and Trigka (2025) [13] mentioned that FL protects privacy by keeping data on your device instead of central server. This helps meet security laws e.g., General Data Protection Regulation (GDPR) without moving sensitive information.

**Cybersecurity:** The modern era of digital transformation has reshaped society's function and moved to global hyper-connectivity. This evolution is marked by shift from PC era to current age of AI and Cloud Computing (Prangon and Wu, 2024) [30]. These not only democratize information but also create vast vulnerabilities across digital ecosystem (Qudus, 2025) [31]. The digital ecosystem comprises interconnected technologies (e.g., AI, cloud computing and e-governance platforms) to provide a wide range of services to the country's beneficiaries (Atuhaire and Kimani, 2025) [6]. Indian government initiatives i.e., Digital India venture, Aadhaar and UPI have accelerated financial inclusion and governance. Besides smooth execution, rapid digitalization has exposed critical cybersecurity and ethical threats in India (Shairgojri and Dar, 2022) [39]. Mohsin (2022) [24] described cybersecurity as branch of data privacy concerned with safeguarding data and information from unauthorized access or hacking using malicious software. Amirkhanova *et al.* (2024) [4] stated that cloud computing has security risks that need strong protection. To fix this, they use lattice-based cryptography based on the Short Integer Solution (SIS).

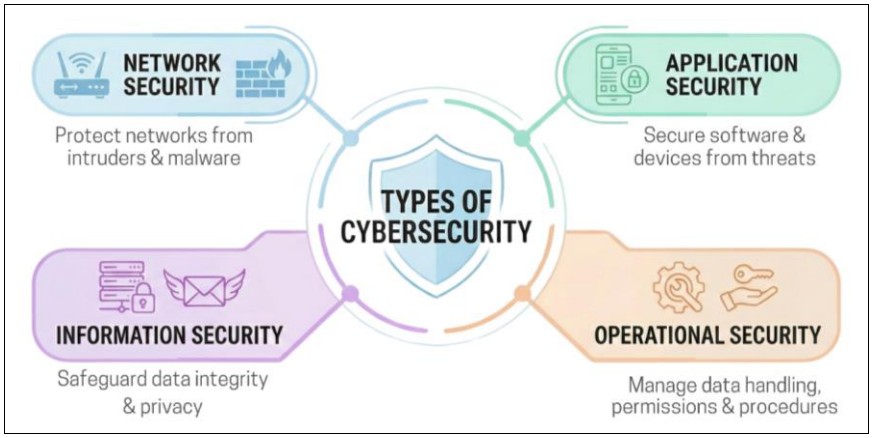


**Fig 1:** Types of Cyber Security

### Aspects of Cybersecurity

Cybersecurity threats are diverse e.g., malware, spyware, and viruses (Pal, 2025) [28]. These threats are often designed to damage or gain unauthorized access to an individual's system for offensive and criminal activities (Shairgojri and Dar, 2022) [39]. Phishing is usually executed by email to steal personal and sensitive data. An example of such threat includes cyberattacks aimed at government agencies and financial institutions. It uses ransomware to lock systems until fee is paid. Additionally, misinformation circulated through social media has emerged as ethical cyber threat that influences public opinion and government or private ventures.

To cope with Cybersecurity threats, we need to develop an effective multifaceted cybersecurity approach. Cybersecurity needs balanced approach towards technical pillars *viz*., confidentiality, Integrity, and availability (Pal, 2025) [28]. It is collectively referred to as CIA (Confidentiality Integrity Availability). Further, ethical and emerging aspects including data privacy, algorithm bias and transparency, are also critical aspects of cybersecurity (Awosika *et al.*, 2024) [7].

**Cyber-privacy:** Privacy is right of an individual so that their personal data has proper handling, processing, and storage. It ensures that data is used lawfully and the user has control over it. Cyberprivacy differs from cybersecurity. Cybersecurity deals with protecting data from unauthorized access, whereas cyberprivacy maintains rights of individuals to control their personal information from unauthorized disclosure (Akash *et al.*, 2025) [2]. It can be regulated by implementing data minimization, purpose limitation and the right to be forgotten. Data minimization could be enforced towards collection of only necessary data from users to maintain privacy (Ganesh *et al.*, 2025) [16]. Furthermore, data should be used only for a specific purpose with user's consent. It cannot be reused or shared without new consent from user. The user has the right to be forgotten, meaning they can request that web platforms permanently delete their data from servers.

**Privacy by Design (PbD):** Modern cybersecurity frameworks adopt PbD. It is a proactive approach where privacy is embedded into IT architecture from commencement of the service (Andrade *et al.*, 2022) [5]. It relied on seven principles of PbD (Fig. 4).

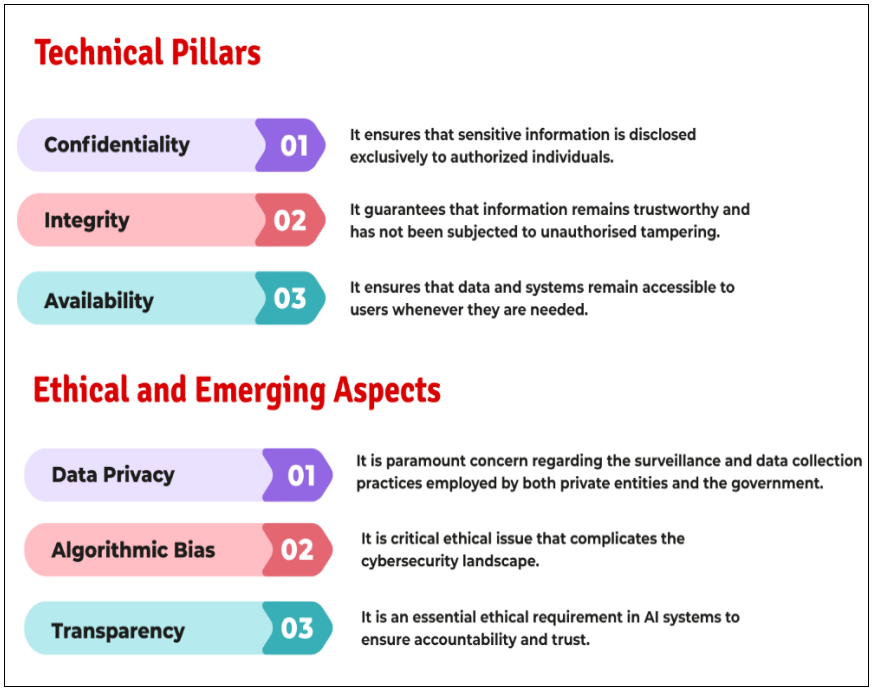


**Fig 2:** Aspects of Cybersecurity threats

**Government Ventures and Policies:** To combat these threats, Governments of India was implemented robust frameworks, as shown in Fig. 3 and Table 1.

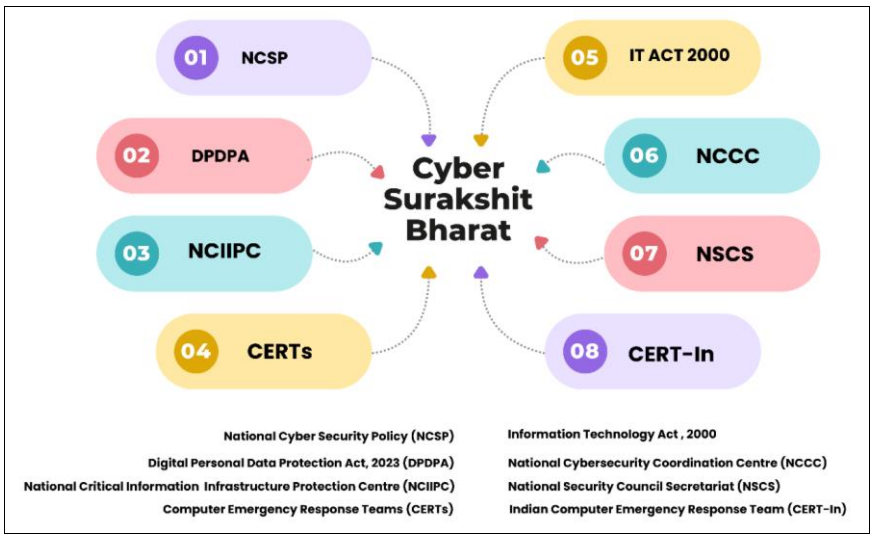


**Fig 3:** Government Ventures and Policies

**Table 1:** List of Entity/Act under Government Ventures and Policies towards cybersecurity

| S. No. | Entity / Act | Type | Remarks | References |
|---|---|---|---|---|
| 1. | NCSP | Policy | It is a strategic framework designed to safeguard public and private infrastructure from cyber-attacks. Its goal is to build a secure and resilient cyberspace for citizens, businesses and government. | Pandey and Parashar (2025) [29] |
| 2. | IT Act, 2000 | Legislation | It is the primary law in India that addresses cybercrime and electronic commerce. It establishes legal framework for electronic governance. | Pandey and Parashar (2025) [29] |
| 3. | DPDPA, 2023 | Legislation | This act focuses on management and processing of digital personal data. It establishes rights of individuals andobligations of data fiduciaries. | Pandey and Parashar (2025) [29] |
| 4. | CERT-In | Organization | The national nodal agency responsible for collecting, analyzing and disseminating information on cyber incidents. It performs emergency response measures. | Chaturvedi and Srivastava (2023) [10] |
| 5. | CERTs | Organization | It refers to a broader network of emergency response teams that manage cybersecurity incidents with CERT-In serving as the national lead. | Chaturvedi and Srivastava (2023) [10] |

| | | | | |
|---|---|---|---|---|
| 6. | NCIIPC | Organization | It is a unit tasked with safeguarding nation's critical information infrastructure (CII), including sectors like power, banking, and transportation, where damage could affect national security or the economy. | Basu (2025) [9] |
| 7. | NCCC | Organization | It is an operational cybersecurity and e-surveillance agency designed to monitor communication metadata and deliver real-time situational awareness. | Rajput (2020) [33] |
| 8. | NSCS | Organization | It is the apex body responsible for addressing the country's political, economic, energy and strategic security issues. It often oversees overall cybersecurity strategy. | Rajput (2020) [33] |

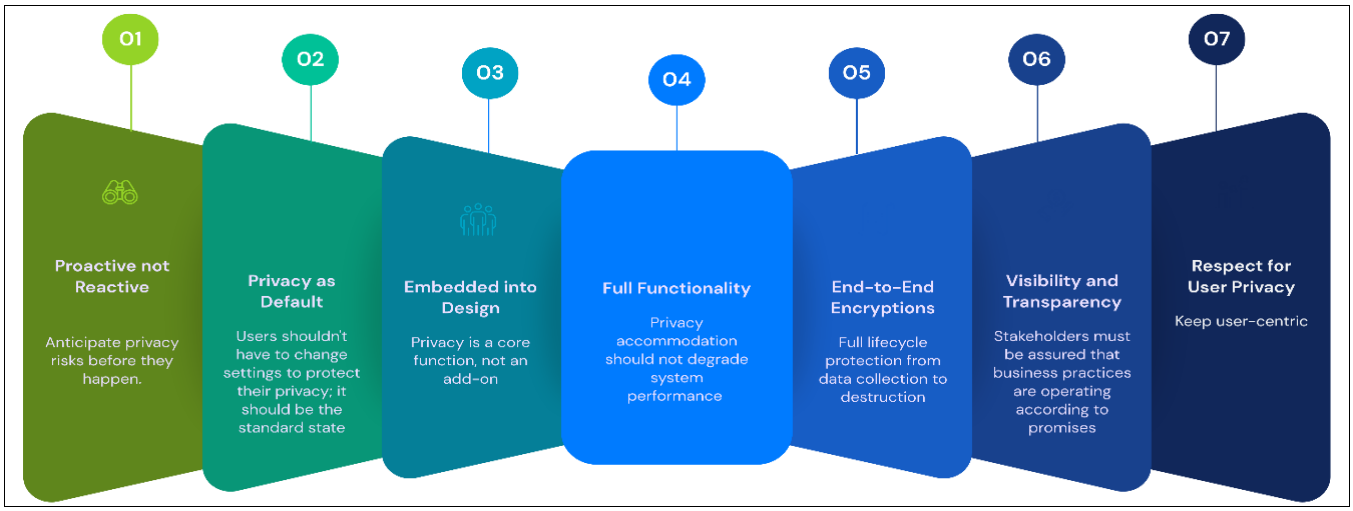


**Fig 4:** Seven principles of PbD

Demelius *et al.* (2025) [12] divulged differential privacy to protect data in machine learning using strong mathematical models for privacy. It can be used against threat and private generative models to protect users data. Furthermore, data breaches, deanonymization and surveillance are significant threats to user privacy in cybersecurity domain. Above them, social engineering currently involves manipulating individuals into voluntarily revealing confidential information from their telephones. However, some Privacy-Enhancing Technologies (PETs) i.e., encryption, tokenization, differential Privacy and Zero-Knowledge proofs, are generally recommended by cybersecurity professionals to enforce privacy (Safa *et al.*, 2022) [38]. The Data Protection Board (DPB) established under DPDPA as quasi-judicial authority to implement privacy laws (Ahmed and Nasir, 2025) [1]. It has role to monitor compliance and investigation of data breaches on data fiduciaries.

**Ethical Prospectives:** Cyberprivacy and Cybersecurity ethics are set of moral principles *viz.*, honesty, trust, confidentiality, integrity and accountability (Michael *et al.*, 2025) [21]. Malicious actors and cybercriminals are usually exploit data for personal gain, but responsible professionals secure data to keep it safe. Surveillance ensures justified, proportional and transparent use of personal data of users. Ethical cybersecurity relies on four aspects (Fenech *et al.*, 2024) [14]. First is data privacy which requires strict protection of personal information. Second is informed consent that requires always obtaining permission before collecting any data. Third is fair use ensures that technology is used in a way that helps everyone equally. Finally, preventing misuse of users data from powerful tools like AI. Together, these actions build trust and keep the digital world safe.

**AI Ethics and Governance:** An effective AI ethics framework is needed to prioritise fairness, accountability and transparency in the digital ecosystem (Awosika *et al.*, 2024) [7]. It ensures automated decisions that do not harm citizens. Moreover, Bias audit systems are essential in AI-based governance, hiring and finance to prevent discrimination against diverse population (Atuhaire and Kimani, 2025) [6]. For instance, recruitment algorithms need to be checked to ensure that they do not unfairly reject candidates on basis of rural Hindi-medium colleges in favor of urban English speakers. Similarly, financial AI models should not deny loans to rural women because they tend to lack formal credit score history in their database. They must be analyze by alternative data like their source of income and potential to pay loans by physical meeting with them. Beyond algorithms, ethical frameworks are also taking care of digital divide and spread of misinformation to protect society. Additionally, digital equality needs to be considered. For example, when designing AI tools that operate on low-cost smartphones, support regional languages and leverage the widespread success of UPI interfaces. Concurrently, there is need to address proliferation of deepfakes, which pose a threat to democracy (Tripathi *et al.*, 2023) [41]. For example, during elections, AI-generated videos of politicians should be explicitly labelled as synthetic to prevent voter manipulation. Currently, criminals are using AI voice cloning to impersonate family members in "Jamtara-style" financial scams (Verma, 2021) [42], which need to be taken into attention by releasing strict legal measures to stop malicious surveillance and fraud.

**Edge, Cloud and Network Security for Connected Environments:** Security in connected environments starts from Edge moves through Network and ends in Cloud (Ometov *et al.*, 2022) [27]. Edge Security is applicable for devices like smart meters or traffic sensors that are vulnerable to physical tampering. These devices seek security which is embedded in hardware itself. Smart Energy Meters in states like Uttar Pradesh use tamper-evident seals and localized encryption (Sahu *et al.*, 2025) [37]. This prevents power theft at source before data even reaches central server. Cloud Security is usually applicable where massive data is stored e.g., DigiLocker that secures millions of documents in the cloud using distinct gateways (Kanungo *et al.*, 2024) [19]. The scrutiny system need to ensures that a breach in one department i.e., transport, does not compromise data in another e.g., education. Network Security protects data in transit e.g., Reliance Jio's 5G rollout allows dedicated "slices" for emergency services (Fue *et al.*, 2025) [15]. This ensures that high network traffic during cricket match does not slow down critical ambulance telemetry data.

**DID and Blockchain in Connected Security**

Traditional identity systems are centralized and hence associated with certain risk factors. If one server is hacked, then millions of identities could be stolen easily. Decentralized Identity (DID) and IOTA (Internet of Things Application)-specific technologies is allow users to own their identity where users phone holds keys and only they can share what is needed (Ramírez-Gordillo *et al.*, 2025) [34]. For instance, Blockchain-based caste certificate issuance in Maharashtra allows citizens to prove their status to a verifier without revealing other personal details. This approach help to prevent data scraping, however it was a proposal, not in released. Further, Blockchain for Integrity creates an unchangeable record of events (Nair *et al.*, 2021) [26]. Telangana's land record system (Dharani) explores blockchain to make property records tamper-proof. This prevents land grabbing by ensuring that once sale is recorded, no corrupt official can retroactively change owner's name. Himdi (2024) [18] endorsed blockchain and AI-driven advanced cybersecurity framework for developing smart cities.

**Human-Driven Security and Awareness**

Technology alone cannot stop cyberattacks. Human error is biggest vulnerability in IoT and smart systems. Attackers target utility workers to gain grid access by using phishing. For instance, hackers might send fake "BSES Bill Update" Short Message Service (SMS) messages to consumers or staff. (Tripathi *et al.*, 2023) [41] Awareness campaigns teach users to verify sender identity before clicking links. These practices prevent malware entry into grid network. The most common threat is to default password risks. The users often leave devices on factory settings e.g., Closed-Circuit Television (CCTV) cameras often use default passwords like admin123. Awareness drives must encourage users to change these credentials immediately to prevent live feeds from being leaked online.

**Cybersecurity for IoT, Smart Cities, and Smart Grids**

Smart cities rely on interconnected sensors. A failure in one sector can cascade into others. IoT devices are often cost-effective and lack built-in security (Taherdoost, 2023) [40]. Botnets can hijack weak devices to attack others. The Indian Computer Emergency Response Team (CERT-In) issues guidelines for IoT device makers (Chaturvedi and Srivastava, 2023) [10]. They require smart bulbs and fridges sold in India to support security patches, ensuring they don't become permanent entry points for hackers. Smart Cities has interconnected traffic, water, and police systems e.g., Pune Smart City sensors collect traffic data to optimize signals (Rehena and Janssen, 2019) [35]. The system is designed to count vehicle types without recording individual license plates, balancing traffic management with driver privacy. Smart power grid is critical national infrastructure. Cyberattacks can cause physical damage by remote disconnection of power and load imbalance. This could be overcome by using air-gapped networks. Mumbai Power Outage 2020 was suspected to be cyber-sabotage. Rihan *et al.* (2023) [36] evaluated meta-learning principles to identify cyberattacks in IoT networks. They have been constructed meta-learner model by using Deep Learning models including Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM) and Convolutional Neural Network (CNN). Subsequently, they have been used Logistic Regression, Multi-Layer Perceptron (MLP), Support Vector Machine (SVM) and XGBoost to identify the attacks based on those predictions. They evaluated this approach with IoT dataset of 2020 and found that XGBoost model performed with 98.75% accuracy and 98.30% precision. Recently, Rahmati and Pagano (2025) [32] revealed Federated Learning-Driven Cybersecurity Framework (FLDCF) for real-time threat detection capabilities of IoT networks.

**Conclusion**

The future of cybersecurity would be defined by the competition between cybersecurity and cyberattacks. AI serves as a double-edged blade, as it can automate threat detection and response accordingly in one side. Whereas it also allows cybercriminals to launch more sophisticated and automated attacks on the other side. The rapid expansion of the IoT and cloud computing will exponentially increase the risk of cyber-attack. It will demand decentralized security solutions e.g., blockchain. The prime concern would be "Cyber Resilience". We need not just defend against attacks, but also be concerned to recover quickly to continue operations during breach. Therefore, we need to implement strong regulatory measures in response to deepfakes and cybercriminals to ensure ethical cyberpractices.

**Acknowledgement**

The author would like to express gratitude to Grammarly for its assistance in ensuring the correct spelling, grammar, and tone of manuscript. Furthermore, acknowledgement is extended to Canva for designing the figures.

**References**

1. Ahmed S, Nasir M. Digital personal data protection act, 2023: A critical analysis. Indian Stud Rev. 2025;6(1):1-20. Available from: https://www.cspgindia.com/_files/ugd/b59e98_a1592c30ede04693ac6400344fee99e1.pdf
2. Akash TR, Sany NJ, Akter L, Sarna SA. Privacy-preserving technique in cybersecurity: Balancing data protection and user rights. J Comput Sci Technol Stud. 2025;7(4):248-263. doi:10.32996/jcsts.2025.7.3.90

3. Alalhareth M, Hong SC. Enhancing the Internet of Medical Things (IoMT) security with meta-learning: A performance-driven approach for ensemble intrusion detection systems. Sensors (Basel). 2024;24(11):3519. doi:10.3390/s24113519
4. Amirkhanova DS, Iavich M, Mamyrbayev O. Lattice-based post-quantum public key encryption scheme using ElGamal's principles. Cryptography. 2024;8(3):31. doi:10.3390/cryptography8030031
5. Andrade VC, Gomes RD, Reinehr S, Freitas CODA, Malucelli A. Privacy by design and software engineering: A systematic literature review. Proc XXI Braz Symp Softw Qual. 2022:1-10.
6. Atuhaire C, Kimani GN. AI and governance: Opportunities and risks of machine learning in public sector decision-making. Eng Technol J. 2025;10(10). doi:10.47191/etj/v10i10.19
7. Awosika T, Shukla RM, Pranggono B. Transparency and privacy: The role of explainable AI and federated learning in financial fraud detection. IEEE Access. 2024;12:64551-64560. doi:10.1109/ACCESS.2024.3394528
8. Baqer M. Energy-efficient federated learning for Internet of Things: Leveraging in-network processing and hierarchical clustering. Future Internet. 2024;17(1):4. doi:10.3390/fi17010004
9. Basu A. India's cyber resilience: Strategy, financing, and collaboration. Asia Policy. 2025;20(2):10-24. doi:10.1353/asp.2025.a960039
10. Chaturvedi S, Srivastava H. The constitutionality of the new Indian CERT-In VPN rules. Int Data Priv Law. 2023;13(4):331-337. doi:10.1093/idpl/ipad015
11. Cooper DS. Before Facebook and Twitter: The online computing revolution of the 1980s [doctoral dissertation]. Liberty University; 2023. Available from: https://digitalcommons.liberty.edu
12. Demelius L, Kern R, Trügler A. Recent advances of differential privacy in centralized deep learning: A systematic survey. ACM Comput Surv. 2025;57(6):1-28. doi:10.1145/3712000
13. Dritsas E, Trigka M. Federated learning for IoT: A survey of techniques, challenges, and applications. J Sens Actuator Netw. 2025;14(1):9. doi:10.3390/jsan14010009
14. Fenech J, Richards D, Formosa P. Ethical principles shaping values-based cybersecurity decision-making. Comput Secur. 2024;140:103795. doi:10.1016/j.cose.2024.103795
15. Fue J, Gutierrez JA, Donoso Y. Understanding security vulnerabilities in private 5G networks: Insights from a literature review. Future Internet. 2025;17(11):485. doi:10.3390/fi17110485
16. Ganesh P, Tran C, Shokri R, Fioretto F. The data minimization principle in machine learning. In: Proc 2025 ACM Conf Fairness Account Transparency; 2025. p. 3075-3093. doi:10.1145/3715275.3732195
17. Ghadi YY, Mazhar T, Shah SFA, Haq I, Ahmad W, Ouahada K, *et al.* Integration of federated learning with IoT for smart cities applications, challenges, and solutions. PeerJ Comput Sci. 2023;9:e1657. doi:10.7717/peerj-cs.1657
18. Himdi T. A blockchain and AI-driven security framework for enhancing cybersecurity in cognitive cities. Adv Artif Intell Mach Learn. 2024;4(4):2908-2925.
19. Kanungo K, Khatoliya R, Arora V, Bari A, Bhattacharya A, Maity M, *et al.* How many hands in the cookie jar? Examining privacy implications of popular apps in India. In: Proc IEEE EuroS&P; 2024. p. 741-757. doi:10.1109/EuroSP60621.2024.00046
20. Korn J. 50 years ago, he made the first cell phone call. CNN Business. 2023 Apr 3. Available from: https://edition.cnn.com
21. Michael K, Herold R, Roussos G. Security and regulation: Cybersecurity, privacy, and trust protecting information and ensuring responsible technology use. Comput Secur. 2025;104804. doi:10.1016/j.cose.2025.104804
22. Mishra DA, Jha GK, Gupta N. Unlocking digital payments: The role of QR codes in India's digital payment revolution. Int J Res Publ Rev. 2024;5(4):9365-9375. doi:10.55248/gengpi.5.0424.1124
23. Mohammadi S, Balador A, Sinaei S, Flammini F. Balancing privacy and performance in federated learning: A systematic literature review on methods and metrics. J Parallel Distrib Comput. 2024;192:104918. doi:10.1016/j.jpdc.2024.104918
24. Mohsin K. Data privacy and cybersecurity. SSRN Electron J. 2022. doi:10.2139/ssrn.4299439
25. Mukherjee R. Jio sparks Disruption 2.0: Infrastructural imaginaries and platform ecosystems in 'Digital India'. Media Cult Soc. 2019;41(2):175-195. doi:10.1177/0163443718818383
26. Nair SM, Ramesh V, Tyagi AK. Issues and challenges (privacy, security, and trust) in blockchain-based applications. In: Advances in Data Mining and Database Management. Hershey (PA): IGI Global; 2021. p. 196-209. doi:10.4018/978-1-7998-3295-9.ch012
27. Ometov A, Molua OL, Komarov M, Nurmi J. A survey of security in cloud, edge, and fog computing. Sensors (Basel). 2022;22(3):927. doi:10.3390/s22030927
28. Pal PK. Cybersecurity, privacy, and ethical challenges in India's digital ecosystem. Int J Creat Res Thoughts. 2025;13(5):249-256.
29. Pandey MT, Parashar N. Policy and politics of the digital: Technological and regulatory trajectory in India. Kashmir J Soc Sci. 2025;13(1):1-29.
30. Prangon NF, Wu J. AI and computing horizons: Cloud and edge in the modern era. J Sens Actuator Netw. 2024;13(4):44. doi:10.3390/jsan13040044
31. Qudus L. Advancing cybersecurity: Strategies for mitigating threats in evolving digital and IoT ecosystems. Int Res J Mod Eng Technol Sci. 2025;7(1):3185.
32. Rahmati M, Pagano A. Federated learning-driven cybersecurity framework for IoT networks with privacy preserving and real-time threat detection capabilities. Informatics. 2025;12(3):62. doi:10.3390/informatics12030062
33. Rajput B. Integrated cyber crime and cyber security model. In: Cyber Economic Crime in India. Cham: Springer; 2020. p. 227-260. doi:10.1007/978-3-030-44655-0_10
34. Ramírez-Gordillo T, Maciá-Lillo A, Pujol FA, García-D'Urso N, Azorín-López J, Mora H. Decentralized

identity management for Internet of Things devices using IOTA blockchain technology. Future Internet. 2025;17(1):49. doi:10.3390/fi17010049
35. Rehena Z, Janssen M. The smart city of Pune. In: Smart City Emergence. Amsterdam: Elsevier; 2019. p. 261-282. doi:10.1016/B978-0-12-816169-2.00012-2
36. Rihan SDA, Anbar M, Alabsi BA. Meta-learner-based approach for detecting attacks on Internet of Things networks. Sensors (Basel). 2023;23(19):8191. doi:10.3390/s23198191
37. Sahu SK, Kumar S, Anushka, Panigrahi A. Optimizing QR code security: Best practices and anti-tampering strategies. SN Comput Sci. 2025;6(7). doi:10.1007/s42979-025-04431-1
38. Safa NS, Mitchell F, Maple C, Azad MA, Dabbagh M. Privacy enhancing technologies (PETs) for connected vehicles in smart cities. Trans Emerg Telecommun Technol. 2022;33(10). doi:10.1002/ett.4173
39. Shairgojri AA, Dar SA. Emerging cyber security: India's concern and threats. Int J Inf Technol Comput Eng. 2022;24:17-26. doi:10.55529/ijitc.24.17.26
40. Taherdoost H. Security and Internet of Things: Benefits, challenges, and future perspectives. Electronics. 2023;12(8):1901. doi:10.3390/electronics12081901
41. Tripathi I, Askari N, Yadav A. Cyber security: The making of an international society in the digital age. Communicator. 2023;58(1-2):39-48.
42. Verma A. Phishing in the ocean of deceit: Review of the series Jamtara: Sabka Number Ayega. Media Asia. 2021;48(4):384-386. doi:10.1080/01296612.2021.1971915
43. Wang S, Asif M, Shahzad MF, Ashfaq M. Data privacy and cybersecurity challenges in the digital transformation of the banking sector. Comput Secur. 2024;147:104051. doi:10.1016/j.cose.2024.104051