

“DATA SECURITY AND GOVERNANCE CHALLENGES IN INDIA’S DIGITAL GST ECOSYSTEM”

Dr. Jyoti Agarwal¹, Dr. Gaurav Vishwakarma²

Associate Professor, CAFS, Saudi Electronics University, Saudi Arabia¹

Research Associate, IDC INDIA INNOVATION DEVELOPMENT COUNCIL, New Delhi²

¹Email: j.agarwal@seu.edu.sa, ² dr.gaurav@idcindia.net

Author Note

Dr. Jyoti Agarwal, Email: j.agarwal@seu.edu.sa, <https://seu.edu.sa/en>

Dr. Gaurav Vishwakarma, Email: dr.gaurav@idcindia.net, <https://www.idcindia.net/our-team>

We have no conflict of interest to disclose.

Correspondence concerning this article should be addressed to name, institution, and postal address. Email: email address

ABSTRACT

India’s Goods and Services Tax (GST), managed by the Goods and Services Tax Network (GSTN), represents a significant technology-driven tax reform. While digitalization has increased transparency and compliance, it has also introduced new risks to data security, privacy, and governance. This paper contends that the main challenge for India’s digital GST system is to identify and address its structural, technological, and regulatory weaknesses. Achieving long-term success will require reducing threats like cyberattacks, data breaches, unauthorized access, identity fraud, and system disruptions through targeted reforms in governance and technology.

This study argues that India’s GST data governance framework urgently needs to address key issues such as data ownership, data sharing between agencies, accountability, and compliance with new data protection standards. It examines whether current cybersecurity tools, such as encryption, audits, and disaster recovery, are enough to protect taxpayer data. The study also highlights the privacy and ethical challenges associated with using AI-driven analytics in the tax system. It concludes by recommending a new, security-focused governance model to protect taxpayer interests and help achieve the goals of GST, in line with the Viksit Bharat 2047 vision.

Keywords: GST, data security, digital governance, GSTN, cybersecurity, India, data privacy

1. Introduction

India introduced the Goods and Services Tax (GST) on July 1, 2017, replacing several indirect taxes like excise duty, service tax, and value-added tax. GST aims to simplify the tax structure, improve compliance, and create a unified national market. The system depends on the Goods and Services Tax Network (GSTN), which supports registration, return filing, tax payments, and invoice matching.

Digitalization has enabled taxpayers and authorities to share data in real time, improving transparency and helping reduce tax evasion. However, storing large amounts of sensitive data in a single location raises concerns about data security, privacy, and governance. The GST system stores critical information, including business transactions, financial records, tax liabilities, and supply chain data, making it a major target for cyberattacks and unauthorized access.

Advanced technologies such as artificial intelligence (AI) and data analytics in tax compliance raise new privacy concerns. AI can process large amounts of taxpayer data, including sensitive personal and financial information. This poses risks, such as automated profiling, the revelation of patterns not intended for analysis, and reduced human oversight of decisions made based on this data. These problems make it more likely that people lose control over their personal information, showing the need for strong privacy protections.

This paper first examines the main data security and governance challenges in India’s digital GST system. It then examines how these issues affect taxpayer protection and system integrity, and finally proposes specific policy and technology solutions to strengthen the system.

2. Literature Review

2.1 Digital Transformation of India’s Tax System

GST transformed India’s indirect tax system into a digital platform. The GSTN allows users to register, file returns, match invoices, and pay taxes online. This digital approach has made tax administration more efficient, reduced paperwork, and increased transparency.

However, adopting technology has also introduced new challenges. Studies report issues such as system downtime, server overload during peak filing periods, and technical problems that disrupt compliance.

2.2 Data Security Risks in the GST Ecosystem

The GST system manages and stores large amounts of financial and transaction data from businesses across India. Storing all this data in a single location increases the risk of cyberattacks, data breaches, and unauthorized access.

India has experienced a surge in cybersecurity incidents in recent years, such as the 2020 cyberattack on the Kudankulam Nuclear Power Plant and the 2021 data breach involving the Domino’s India database, which exposed sensitive customer information. These incidents exemplify the growing threats to digital government platforms and highlight vulnerabilities in critical digital infrastructure.

Common data security risks include:

- i. Data breaches and hacking
- ii. Insider threats and unauthorized data access
- iii. System vulnerabilities and malware attacks
- iv. Phishing and identity theft targeting taxpayers

2.3 Privacy and Data Governance Concerns

Recent literature consistently identifies privacy concerns as a major challenge in the use of big data analytics and AI for tax compliance monitoring. The Journal of Informatics Education and Research (2025) emphasizes that AI-powered systems facilitate automatic profiling and algorithmic decision-making with limited human oversight, resulting in

granular taxpayer profiles generated from both personal and financial data patterns. Synthesizing existing studies, critics warn that these tools heighten the risk of discriminatory outcomes, inadvertent privacy violations, and pervasive surveillance, while academic proponents highlight the effectiveness of advanced analytics in promoting compliance and detecting fraudulent activity. Drawing on this body of research, it is evident that resolving the tension between increased enforcement enabled by AI and the protection of individual rights is a persistent and complex issue, particularly given that AI systems may use or share personal information in ways not previously communicated to individuals.

India passed the Digital Personal Data Protection Act (DPDP) in 2023, establishing a consent-based framework for the collection and use of data. However, challenges remain in implementing the law and clarifying the rules governing digital governance.

3. Research Objectives

This study aims to:

- a) Identify key data security risks in India’s digital GST ecosystem.
- b) Examine governance challenges associated with digital tax administration.
- c) Analyse the impact of technological and regulatory gaps on taxpayer data protection.
- d) Propose policy and technological solutions to improve data security and governance.

4. Methodology

This research adopts a qualitative approach utilizing secondary data sources. Data were collected using specific selection criteria, including the relevance, credibility, and recency of the sources to ensure a comprehensive and current representation of the subject matter. Sources were chosen based on their scholarly merit, policy significance, or direct relevance to India’s GST digital infrastructure, data security, and governance challenges. Data has been collected from:

- i. Academic research papers

- ii. Government reports
- iii. Policy documents
- iv. Industry publications
- v. Journals and scholarly articles

The study applies a rigorous qualitative review methodology, systematically analysing and synthesizing existing literature on GST’s digital infrastructure, cybersecurity risks, and digital governance in India. This approach is grounded in predefined selection criteria and thematic coding to ensure methodological transparency and reproducibility. Through this framework, the study identifies core themes and critically evaluates the effectiveness of various strategies and interventions documented in the sources.

Following the methodology, this section explains the main data security challenges the GST system faces today.

The GSTN platform stores massive amounts of sensitive data, including:

- a) Taxpayer financial records
- b) Business transactions
- c) Supply chain information
- d) Bank details

Centralized data storage is an appealing target for cybercriminals and other bad actors. One breach could reveal the confidential data of millions of taxpayers.

5.2 Cybersecurity Threats

India has experienced a significant increase in cyberattacks targeting digital infrastructure. Digital government platforms handling financial data are particularly vulnerable to cyber threats such as:

- i. Distributed Denial of Service (DDoS) attacks
- ii. Malware infiltration

- iii. Ransomware attacks
- iv. Phishing scams targeting taxpayers

These threats can endanger both government systems and taxpayer information.

Infrastructure Limitations

The GSTN portal has faced technical issues, including:

- a) Server crashes during peak filing periods.
- b) Slow response times
- c) System downtime
- d) Data synchronization errors

These technical problems can disrupt tax filing and lower trust in the system.

5.4 Data Integration and Interoperability Issues

The GST system interacts with multiple government databases, such as:

- I. Income tax systems
- II. Customs data
- III. Banking systems

However, differences in data formats and limited ability for these systems to work together make data analysis and compliance monitoring difficult.

6. Governance Challenges

6.1 Regulatory and Legal Gaps

India’s data governance framework is still growing. The Digital Personal Data Protection Act provides a legal foundation, but there are still concerns about enforcement, oversight, and transparency in data collection and use. For example, the Act requires consent for data processing, but it does not provide clear rules for authorities to audit or monitor compliance in complex systems such as the GST Network. This creates uncertainty about how violations will be found and fixed.

- i. How the government uses the data
- ii. Data retention policies
- iii. Access control mechanisms

If transparency is lacking, people may lose trust in digital government systems.

6.3 Digital Divide and Capacity Constraints

Many small businesses and rural taxpayers lack the digital skills or infrastructure to use the GST platform effectively. This digital gap makes compliance more difficult and increases the risk of errors.

6.4 Institutional Coordination

The GST ecosystem involves coordination among multiple agencies, including:

- Central Board of Indirect Taxes and Customs (CBIC)
- State tax departments
- GST Network (GSTN)

Fragmented governance can lead to coordination problems and less efficient data management.

7. Policy and Technological Recommendations

This section brings together the study’s findings on security and governance challenges in the digital GST system and turns them into specific policy and technology recommendations. These suggestions aim to fix ongoing weaknesses that threaten data security, privacy, and the system’s integrity. The proposals are designed to reduce risks, build public trust, and ensure the GST system meets both regulatory and technical standards.

7.1 Strengthening Cybersecurity Infrastructure

Government agencies should implement:

- Advanced encryption protocols
- Multi-factor authentication for system access

- Continuous vulnerability assessments
- AI-based threat detection systems

Multi-factor authentication has already been introduced to strengthen security on the GST portal.

7.2 Enhancing Data Protection Frameworks

India should strengthen data protection by:

- Establishing independent data protection authorities
- Implementing strict data access controls
- Defining clear data retention and sharing policies

7.3 Adopting Emerging Technologies

Technologies like blockchain can improve transparency, traceability, and security in tax systems by creating tamper-resistant records.

7.4 Improving Digital Literacy and Infrastructure

Government initiatives should focus on:

- * **Training programs for small businesses**
- * **Simplifying GST compliance procedures**
- * **Improving internet infrastructure in rural areas**

8. Conclusion

India’s digital GST system is one of the world’s largest technology-based tax platforms and has greatly improved transparency and compliance. However, it now faces major challenges in data security, privacy, and governance that are crucial for its future success and sustainability.

The identification of significant risks arising from centralized GST data, increasing cyber threats, technical limitations, and evolving regulatory frameworks underscores the need for immediate and focused policy interventions. These findings demonstrate that

policymakers must prioritize robust cybersecurity measures, enact comprehensive data protection regulations, strengthen governance frameworks, and facilitate the integration of emerging technologies into the GST infrastructure. Such policy actions are not only critical to effectively mitigating systemic vulnerabilities but also to safeguarding taxpayer rights and sustaining public trust in digital tax administration.

By focusing on data security and improved governance, India can ensure its digital GST system remains strong, efficient, and trustworthy. This will help build a secure base for the country’s ambitious digital future.

References

1. (2021). India: Kushinagar Airport declared as a Customs Notified Airport. MENA Report, (),
2. Andhra Govt to introduce Biometric Face Authentication for GST registration.<https://www.newindianexpress.com/states/andhra-pradesh/2025/Jan/01/andhra-govt-to-introduce-biometric-face-authentication-for-gst-registration>
3. Disabling the Router Firewall: A Practical Guide to Last Resort. <https://www.internetsafetystatistics.com/disabling-router-firewall-guide/>
4. Drishti IAS (2025). Data Governance Challenges in India.
5. Drone Services Market to be Valued at USD 16 Billion in 2023 & Set to Thrive at a CAGR of 28.5% During 2025-30. <https://www.marknteladvisors.com/press-release/drone-services-market-growth>
6. Government of India. GST Network Reports.
7. Grant Thornton Bharat (2024). Cybersecurity and Governance Challenges.
8. IJFMR (2026). Digital Infrastructure and GST Implementation Issues.
9. JETIR (2025). Cybersecurity Risks in GSTN Infrastructure.

10. Journal of Informatics Education and Research (2025). AI and Data Privacy in Tax Systems.
11. Legal Solution – Redback. <https://redback.net/gst-it-filings.php>
12. Lima, V., & Gaspar, F. C. (2025). Milton Friedman's economic theory in the age of platform capitalism and AI. STUDIES IN SOCIAL SCIENCES REVIEW. <https://doi.org/10.54018/sssrv6n1-021>
13. Putri, S. L. K., & Hasmarini, M. I. (2025). ANALISIS PENGARUH RATA-RATA LAMA SEKOLAH, ANGKA HARAPAN HIDUP, PENGANGGURAN, DAN INDEKS PEMBANGUNAN MANUSIA TERHADAP TINGKAT KEMISKINAN DI PROVINSI JAWA TIMUR (2019-2023). <https://doi.org/10.31539/costing.v8i3.14763>
14. R, N. T. (2026). Data-Driven Governance in GST: Leveraging Big Data for Tax Compliance Monitoring. Zenodo (CERN European Organization for Nuclear Research). <https://doi.org/10.5281/zenodo.19500215>
15. Reducing Inventory Costs with Effective Demand Forecasting. <https://k3s.com/en/articles/reducing-inventory-costs-with-effective-demand-forecasting>
16. Shahnawaz, K. (2024). ADAPTIVE CYBERSECURITY STRATEGIES FOR CLOUD-BASED REAL-TIME DATA ANALYTICS PLATFORMS. <https://core.ac.uk/download/653452450.pdf>
17. Shome, P. (2018). Goods and Services Tax (GST). RePEc: Research Papers in Economics. <https://ideas.repec.org/p/ess/wpaper/id12765.html>
18. Top 3 FHIR Servers by Security Frameworks, Access Control, and Audit Capabilities: Aidbox, Smile Digital Health, Microsoft Azure <https://doubleshotreviews.com/clinical-software/top-3-fhir-servers-by-security->

frameworks-access-control-and-audit-capabilities-aidbox-smile-digital-health-
microsoft-azure/