

# **Cybersecurity in Property Transactions- Protecting digital land records from fraud and data breaches**

**Sree Lekha. V<sup>1</sup>**

**Divya Rajan<sup>2</sup>**

**Shivya Lakshmi. M<sup>3</sup>**

## **Abstract:**

Real estate in India is a significant sector that drives the country's economic growth, particularly its GDP. Foreign direct investment in real estate has risen. It is expected to increase tenfold. Land administration and management vary in language, culture, region, topography, nomenclature, and socio-economic factors. In this context, accurate and updated digital land records are essential. These records must be easily accessible online by the public. The Digital India Land Records Modernisation Programme was launched in 2016. It aims to modernize land record management, reduce land/property disputes, and enhance transparency. The earlier National Land Records Modernization Programme (NILRMP) was approved in 2008 as a centrally sponsored scheme. It was later revamped as the Digital India Land Records Modernization Programme (DILRMP), a central sector scheme with full central government funding effective from April 1, 2016. The scheme has been extended from 2021-22 to 2025-26 with an outlay of Rs. 875 crores. It now includes computerization of all revenue courts with integration to land records and consent-based Aadhaar linking with Records of Rights (RoR). This paper discusses measures to protect digital land records from fraud and breaches. Ultimately, digitalization must balance efficiency with legal safeguards. It must uphold citizens' property rights while leveraging technology for seamless governance.

Keywords: Real estate, Land Records, Breach, Digitalisation, Technology

---

<sup>1</sup> Sree Lekha. V, Assistant Professor, Vels School of Law, [sreelekhavelu2022@gmail.com](mailto:sreelekhavelu2022@gmail.com).

<sup>2</sup> Divya Rajan, Assistant Professor, Vels School of Law, [divyarajan2329@gmail.com](mailto:divyarajan2329@gmail.com).

<sup>3</sup> Shivya Lakshmi. M, Assistant Professor, Vels School of Law, [L8shivya@gmail.com](mailto:L8shivya@gmail.com).

## 1. INTRODUCTION

Land constitutes one of the most valuable immovable assets and forms the backbone of economic development, social stability, and individual security. In India, land ownership is not merely a proprietary interest, but also a source of livelihood, social identity, and political power. Consequently, land records play a critical role in determining ownership, facilitating transactions, resolving disputes, and enabling access to credit.

Traditionally, land records in India were maintained manually by revenue authorities in physical registers. These records were often plagued by inaccuracies, delays, lack of transparency, and susceptible to manipulation issues such as fraudulent entries, destruction of records, and bureaucratic inefficiencies, which were common, leading to widespread litigation and disputes.<sup>4</sup>

To address these challenges, the Government of India introduced digitalization initiatives under the Digital India Land Records Modernisation Programme. The objective was to create a unified, transparent, and accessible system of land records for computerisation, integration of textures and spatial data, and real-time updating mechanisms.<sup>5</sup> While digitalization has significantly improved accessibility and reduced manual errors, it has simultaneously introduced new vulnerabilities in the form of cyber threats, data breaches, and digital fraud.

The digital or legal implications of these developments are profound. Digital land records now contain sensitive personal and proprietary information, making them attractive targets for cyber criminals. Unauthorised access or manipulation of such records can result in fraudulent transfers, identity theft, and large-scale financial losses.<sup>6</sup>

Further, the recognition of the right to privacy as a fundamental right by the Supreme Court in *Justice K.S. Puttaswamy vs. Union of India* has imposed a constitutional obligation on the state to ensure data protection and informational privacy<sup>7</sup>. This development underscores the need for a robust legal framework that not only governs property transactions but also safeguards digital data.

---

<sup>4</sup> NITI Aayog, *Land Records and Titles in India* (2020).

<sup>5</sup> Ministry of Rural Development, *Digital India Land Records Modernization Programme (DILRMP) Guidelines* (2016).

<sup>6</sup> World Bank, *Land Governance Assessment Framework* (2019)

<sup>7</sup> *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India).

Therefore, the intersection of property law information, technology, law, and data protection law becomes crucial in addressing the challenges posed by digital land records. This paper seeks to analyse these legal dimensions and evaluate the adequacy of existing frameworks.

## **2. Evolution of Digital Land Records**

### **2.1 Traditional Land Record Systems**

Historically, India followed a decentralised system of land record maintenance, where village-level officials such as patwaris were responsible for recording land ownership and transactions. These records included documents such as the Record of Rights, tenancy records and cadastral maps. However, the manual nature of these systems made them vulnerable to human error, tampering and corruption.<sup>8</sup>

Additionally, the absence of a conclusive titling system meant that land records served only as presumptive evidence of ownership rather than definitive proof. This often resulted in overlapping claims and prolonged litigation.

### **2.2 Transition to digital systems**

Recognising these limitations, the Government of India initiated several reforms, culminating in the DILRMP. The programme aims to digitalise textual and spatial land records and integrate registration and mutation processes. Establish a transparent and accessible land information system.

Digitalisation has enabled online access to land records, reduced transaction costs and improved administrative efficiency.<sup>9</sup> However, the transition has not been without challenges. Many states digitalised existing records without verifying their accuracy, thereby perpetuating historical errors in digital form.

### **2.3. Legal Implications of Digitisation**

The digitalisation of land records raises several legal issues. First, the continued reliance on a presumptive title system undermines the reliability of digital records. Second, the integration of land records with digital platforms introduces concerns regarding data authenticity, integrity and security.

---

<sup>8</sup> Government of India, *Report on State of Land Records* (2018).

<sup>9</sup> Ministry of Rural Development, *DILRMP Progress Report* (2022).

Moreover, the legal recognition of electronic records under the Information Technology Act, 2000, provides validity to digital land records.<sup>10</sup> However, the absence of a comprehensive legal framework, specifically addressing digital land governance, creates ambiguity in cases of disputes and fraud.

Thus, while digitalisation represents a significant advancement, it must be accompanied by legal reforms to ensure accuracy, reliability and security.

### **3. Nature of Fraud in Digital Land Records**

The digitalization of land records, while beneficial, has created new avenues for fraudulent activities. These frauds exploit both technological vulnerabilities and legal loopholes.

#### **3.1. Identity theft and impersonation**

One of the most common forms of fraud involves the impersonation of landowners.

Fraudsters use forged identity documents or stolen credentials to gain access to digital systems and execute unauthorised transactions.<sup>11</sup> The lack of robust authentication mechanisms exacerbates this issue.

#### **3.2. Unauthorised data manipulation**

Digital systems are susceptible to unauthorised alteration of data. Hackers or insiders may manipulate land records to change ownership details, modify boundaries, or create fictitious entries. Such alterations can be difficult to detect and may result in wrongful transfers of property.

#### **3.3. Insider Fraud**

Officials with authorised access to land record systems may misuse their privileges to manipulate records for personal gain. Insider threats are particularly dangerous because they involve individuals with knowledge of system vulnerabilities.<sup>12</sup>

#### **3.4. Fraudulent transactions**

Digital platforms facilitate faster transactions, but they also enable fraudulent transfers through forged documents and manipulated records. The lack of real-time verification mechanisms increases the risk of such fraud.

---

<sup>10</sup> Information Technology Act, No. 21 of 2000, § 4 (India).

<sup>11</sup> K. Ramesh, *Cyber Fraud in Land Transactions*, 45 *J. Indian L. Inst.* 123 (2021).

<sup>12</sup> OECD, *Insider Threats in Public Institutions* (2020).

### **3.5. Systematic and organised fraud**

In some cases, fraud is carried out on a large scale involving multiple actors, including officials, intermediaries, and cybercriminals. These schemes exploit systematic weaknesses and a lack of coordination between different authorities.

The legal framework must address these diverse forms of fraud by incorporating stringent penalties, robust authentication mechanisms, and accountability measures.

## **4. Cybersecurity Threats and Data Breaches**

### **4.1 Nature of Cyber Threats**

Digital land record systems are exposed to a wide range of cybersecurity threats, including hacking, phishing, malware, attacks, and ransomware. These threats can compromise the confidentiality, integrity, and availability of data.<sup>13</sup>

### **4.2 Risk of centralised databases.**

Most digital land record systems rely on centralised databases, which create single points of failure. A successful cyber attack on such systems can lead to large-scale data breaches, affecting millions of records.

### **4.3 Data breaches and their consequences**

Data breaches involving land records can have severe consequences, including.

- \* exposure of sensitive personal information,
- \* identity, theft, and financial fraud,
- \* loss of public trust. In government systems

### **4.4 Legal and constitutional implications**

The Right to privacy recognised in *Puttaswamy Vs Union of India* imposes a duty on the state to protect personal data. Any failure to secure digital land records may amount to a violation of fundamental rights.<sup>14</sup> The Digital Personal Data Protection Act 2023 further strengthens this obligation by requiring data fiduciaries to implement reasonable security safeguards and prevent data breaches.<sup>15</sup>

---

<sup>13</sup> CERT-In, *Cyber Security Threat Report* (2022).

<sup>14</sup> *Puttaswamy*, (2017) 10 SCC 1.

<sup>15</sup> Digital Personal Data Protection Act, No. 22 of 2023 (India).

#### **4.5 Need for a robust cybersecurity framework**

To address these challenges, it is essential to

- \* implement strong encryption and authentication mechanisms
- \* conduct regular security audits
- \* establish incident response systems
- \* ensure compliance with data protection laws.

A comprehensive cybersecurity framework, supported by legal provision is crucial for protecting land records.

#### **5. Legal Framework Governing Digital Land Records:**

The governance of digital land records in India is anchored in a combination of statutory laws, policy initiatives, and administrative mechanisms. At the core lies the Information Technology Act, 2000, which provides legal recognition to electronic records and digital signatures. Sections 43 and 66 of the Act impose civil and criminal liability for unauthorised access, data theft, and hacking, thereby offering foundational protection against digital fraud in land records.

The Registration Act, 1908 and the Transfer of Property Act, 1882, continue to govern the substantive legality of land transactions. While these statutes were originally designed for physical documentation, their integration into digital platforms has allowed states to modernise land registration processes through e-governance initiatives.

A major policy initiative in this domain is the Digital India Land Records Modernisation Programme (DILRMP). This program aims to digitise land records, integrate textual and spatial data, and ensure real-time updation. By reducing human intervention and increasing transparency, DILRMP seeks to minimise fraud such as double registration or tampering of ownership records.

Data protection has recently gained prominence with the enactment of the Digital Personal Data Protection Act, 2023. Although primarily focused on personal data, it has implications for land records as they often contain sensitive personal information. The Act mandates lawful processing, data minimisation, and security safeguards, thereby indirectly strengthening protection against breaches.

Additionally, state-specific land revenue codes and registration rules regulate the maintenance and authentication of digital land records. Many states have introduced blockchain-based pilot projects to enhance immutability and prevent unauthorised alterations.

However, the current framework remains fragmented. There is no single comprehensive statute exclusively governing digital land records. Instead, protection is derived from a patchwork of laws addressing cybersecurity, property rights, and data governance. This creates interpretational challenges and enforcement inconsistencies.

In conclusion, while India has made significant strides in digitising land records through legislative and policy mechanisms, the legal framework is still evolving. A more unified and technology-specific regulatory approach is necessary to ensure robust protection against fraud and data breaches in digital land systems.

## **6. Legal Challenges and Gaps:**

Despite the increasing digitisation of land records, significant legal challenges and gaps persist, as highlighted by judicial decisions. In *Samiullah v. State of Bihar*,<sup>16</sup> the Supreme Court underscored the structural deficiencies in India's land registration system, noting that digitisation alone does not guarantee a clear and marketable title. The Court observed that a substantial portion of civil litigation arises from disputes over land ownership, and the mere conversion of physical records into digital format, without proper title verification mechanisms, may actually aggravate fraud rather than prevent it. This case highlights a fundamental gap in the legal framework—while technology has advanced, the substantive law governing title assurance has not kept pace correspondingly.

Further, large-scale land fraud cases such as the *Gurugram-Manesar Land Scam Case*<sup>17</sup> and *the DLF Land Grab Case*<sup>18</sup> demonstrate how manipulation of land records, administrative discretion, and lack of transparency can facilitate fraudulent transactions. Although these cases originated in a largely pre-digital context, they remain highly relevant, as digitised systems can replicate and even amplify such manipulations if adequate safeguards are not implemented. They reveal a systemic weakness where legal and administrative loopholes allow unauthorised alterations and misuse of land data.

---

<sup>16</sup> *Samiullah v. State of Bihar*, 2025 INSC 1292 (S.C. Nov. 7, 2025)

<sup>17</sup> *Gurugram–Manesar IMT Land Grab Scam Case*, Supreme Court of India, decided on Mar. 13, 2018.

<sup>18</sup> *Belaire Owners' Ass'n v. DLF Ltd.*, Case No. 19 of 2010 (Competition Comm'n of India Aug. 12, 2011).

A major challenge lies in the issue of data integrity. Digital records can be altered through unauthorised access, and proving tampering in court requires technical expertise. The evidentiary value of digital land records, though recognised under the Indian Evidence Act, 1872, often depends on compliance with procedural safeguards such as certification under Section 65B. This creates procedural hurdles and delays in litigation.

Cybersecurity vulnerabilities remain critical. Hackers target government land databases because land data is valuable. Since states lack uniform cybersecurity standards, risks are inconsistent. Although CERT-In issues guidelines, they are not always adopted, increasing the threat to land record security.

Jurisdictional conflicts also pose significant challenges. Land is a State subject under the Constitution, while cybersecurity and data protection fall under the Union's domain. This division often leads to overlapping authorities and a lack of coordination between central and state agencies, weakening enforcement mechanisms.

Moreover, there is a lack of accountability mechanisms for officials managing digital land records. In cases of fraudulent entries or data breaches, fixing liability on government authorities is difficult due to procedural complexities and a lack of clear statutory provisions.

Digital illiteracy and limited access compound the problem. Many rural landowners cannot monitor or verify their records, making them easy targets for fraud. Current laws do not provide effective user protections to address this gap.

Lastly, the absence of robust grievance redressal mechanisms delays dispute resolution. Victims of digital land fraud often face prolonged litigation due to technical complexities and backlog in courts.

In essence, while digitisation has improved efficiency, it has simultaneously introduced new vulnerabilities. Addressing these legal gaps requires a comprehensive statutory framework, stronger cybersecurity norms, and better coordination between authorities.

## **7. Role of Judiciary in Strengthening Legal Protection:**

The judiciary has played a transformative role in strengthening the legal protection of digital land records by interpreting existing laws in light of technological advancements and addressing systemic deficiencies. A significant recent development is reflected in observations by the Supreme Court of India, where it recommended the adoption of advanced technologies such as blockchain to ensure tamper-proof and transparent land record systems.

The Court emphasised that the increasing incidence of land fraud necessitates secure and immutable digital infrastructure, thereby positioning itself not only as an adjudicator but also as a catalyst for policy and technological reform.

Judicial intervention has also been crucial in addressing fraudulent land transactions and administrative irregularities. In the *Sonepat-Kharkhoda IMT Land Case*<sup>19</sup>, the Supreme Court cancelled the land releases and ordered investigations into irregular allocations, reinforcing the principle that state actions affecting land records must adhere to transparency and legality. This case illustrates how the judiciary actively corrects distortions in land governance and ensures accountability of public authorities.

At the doctrinal level, the judiciary has also dealt with broader principles affecting land record systems. In the landmark case of *Frazer v. Walker*<sup>20</sup>, the principle of indefeasibility of title was established, protecting bona fide purchasers even in cases involving prior fraud. While this doctrine promotes certainty in transactions, it also raises concerns in the digital context—if digital land records are compromised, courts may still uphold transactions based on those records, thereby emphasising the need for accuracy and security at the initial stage.

Moreover, courts have consistently upheld the evidentiary validity of electronic records under the Indian Evidence Act, 1872, provided procedural safeguards are met. This has strengthened the legal status of digital land records, enabling their use in dispute resolution. At the same time, the judiciary has expanded the scope of the right to property under Article 300A, treating unauthorised alterations in land records as violations of constitutional rights.

Overall, the judiciary has evolved from a passive dispute-resolution body to an active participant in shaping the legal landscape of digital land governance. Through its judgments and observations, it not only addresses individual cases of fraud but also influences systemic reforms, promotes technological adoption, and reinforces accountability. This proactive role is essential in bridging the gaps left by the legislative framework and ensuring robust protection against fraud and data breaches in digital land records.

## **8. Comparative Legal Perspective:**

A comparative analysis of international practices provides valuable insights into strengthening the legal framework for digital land records in India. Several countries have

---

<sup>19</sup> In re: Sonepat–Kharkhoda Industrial Model Township Land Acquisition Case, (2018) (Supreme Court of India).

<sup>20</sup> *Frazer v. Walker*, [1967] 1 A.C. 569 (P.C.)

adopted advanced legal and technological measures to ensure security, transparency, and reliability.

For instance, Estonia is widely regarded as a global leader in digital governance. Its land registry system operates on blockchain technology, ensuring immutability and protection against unauthorised alterations. The legal framework explicitly recognises digital records as primary evidence, minimising disputes and enhancing trust.

Similarly, Sweden has implemented a blockchain-based land registry system in collaboration with private entities. This system reduces fraud by creating a transparent and tamper-proof record of transactions. Legal provisions ensure strict authentication and verification processes.

In the United Kingdom, the HM Land Registry has embraced digital transformation through secure online platforms. The legal framework emphasises data protection, cybersecurity, and user authentication. The integration of the UK Data Protection Act 2018 ensures robust safeguards against data breaches.

The United States adopts a decentralised approach, with land records maintained at the county level. While this allows flexibility, it also necessitates strong cybersecurity measures. Various states have introduced legislation to address electronic recording and fraud prevention.

These international models highlight the importance of a unified legal framework, advanced technology integration, and strong data protection laws. Compared to these systems, India's approach remains fragmented and less technologically integrated.

Adopting best practices such as blockchain implementation, standardised cybersecurity protocols, and comprehensive legislation can significantly enhance the protection of digital land records in India. A comparative perspective thus underscores the need for reform and modernisation in the Indian legal framework.

## **9. Conclusion**

The digitisation of land records represents a transformative step toward modernising land governance, enhancing transparency, and improving administrative efficiency. However, as this paper has demonstrated, the transition from manual to digital systems has not merely shifted the medium of record-keeping but has fundamentally altered the nature of risks

associated with land administration. Fraudulent activities, once limited to physical manipulation of records, have evolved into sophisticated cyber-enabled offences, while data breaches pose serious threats to both property rights and informational privacy.

The existing legal framework in India—including the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and traditional property laws—provides a fragmented response to these emerging challenges. While these statutes offer partial safeguards, they were not designed to comprehensively address the intersection of land governance, cybersecurity, and data protection. The absence of a dedicated and cohesive legal regime for digital land records creates significant gaps in accountability, liability, and enforcement.

Judicial interventions, particularly in recognising the fundamental right to privacy, have underscored the constitutional imperative to protect personal data and ensure secure digital systems. However, reliance on judicial pronouncements alone is insufficient. There is a pressing need for legislative reform that integrates technological realities with legal principles.

In this context, India can draw valuable lessons from comparative jurisdictions such as the Torrens system and Estonia's digital governance model, which emphasise conclusive titling, state-backed guarantees, and robust technological safeguards. Adopting similar approaches—along with the use of emerging technologies such as blockchain, biometric authentication, and secure digital infrastructure—can significantly enhance the integrity of land record systems.

Ultimately, protecting digital land records requires a multi-dimensional approach that combines legal reform, technological innovation, and institutional accountability. A comprehensive framework must establish clear liability mechanisms, ensure data security, strengthen user authentication, and provide effective remedies for victims of fraud and data breaches. Such measures are essential not only for safeguarding property rights but also for maintaining public trust in digital governance systems.

In conclusion, the future of land governance in India depends on the State's ability to balance technological advancement with legal safeguards. Without a robust and integrated approach, the very systems designed to enhance transparency may become instruments of exploitation. Therefore, strengthening the legal architecture for protecting digital land records is not merely a regulatory necessity but a constitutional and socio-economic imperative.

## References

### A. Statutes and Legislation

- Information Technology Act, No. 21 of 2000.
- Digital Personal Data Protection Act, No. 22 of 2023.
- Transfer of Property Act, No. 4 of 1882.
- Registration Act, No. 16 of 1908 .
- Indian Evidence Act, No. 1 of 1872 .

### B. Cases

- *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
- *Suraj Lamp & Indus. Pvt. Ltd. v. State of Haryana*, (2012) 1 SCC 656.
- *State of Karnataka v. M. Devendrappa*, (2002) 3 SCC 89.

### C. Government Reports & Policy Documents

- NITI Aayog, *Land Records and Titles in India* (2020).
- Ministry of Rural Development, Government of India, *Digital India Land Records Modernization Programme (DILRMP) Guidelines* (2016).
- Ministry of Rural Development, Government of India, *DILRMP Progress Report* (2022).
- Government of India, *Report on the State of Land Records in India* (2018).
- CERT-In, *Cyber Security Threat Report* (2022).

### D. International Reports and Comparative Sources

- World Bank, *Land Governance Assessment Framework* (2019).
- World Bank, *Securing Land Tenure and Property Rights* (2020).
- OECD, *Insider Threats in Public Institutions* (2020).
- Food & Agriculture Organization (FAO), *Land Tenure and Digital Systems* (2021).

### E. Books and Journal Articles

- K. Ramesh, Cyber Fraud in Land Transactions, 45 *J. Indian L. Inst.* 123 (2021).

- Upendra Baxi, *The Future of Human Rights* (3d ed. 2008).
- S. Sivaramakrishnan, Land Governance and Digitalization in India, 12 *Indian J. L. & Tech.* 45 (2020).
- Rahul Matthan, *Privacy 3.0: Unlocking Our Data-Driven Future* (2017).