Page: 1456-1485 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 4 | Issue 2

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.208

© 2026 LawFoyer International Journal of Doctrinal Legal Research

Follow this and additional research works at: www.lijdlr.com
Under the Platform of LawFoyer – www.lawfoyer.in

After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal Legal Research has decided to publish this submission as part of the publication.

In case of any suggestions or complaints, kindly contact (info.lijdlr@gmail.com)
To submit your Manuscript for Publication in the LawFoyer International Journal of Doctrinal Legal Research, To submit your Manuscript Click here

A THEMATIC STUDY ON ELECTRONIC CONTRACTS IN THE DIGITAL AGE: VALIDITY, AUTHENTICATION, AND ENFORCEMENT IN THE INDIAN CONTEXT

M Prakash George[1]

I. ABSTRACT

The rise of digital technology and internet-based commerce has profoundly changed the conventional understanding of contractual relationships in India. E-contracts, or electronic contracts, have emerged as an essential aspect of contemporary business operations, allowing individuals and companies to form agreements via websites, mobile apps, electronic banking services, and online marketplaces. The increasing reliance on digital transactions has heightened the need to comprehend the legal validity, authentication processes, and enforceability of electronic contracts in the Indian legal framework. This study analyzes the legal structure regulating electronic agreements in India, emphasizing the clauses of the Information Technology Act, 2000 and the Indian Contract Act, 1872. It examines how key components of a valid contract, including voluntary consent, lawful consideration, capable parties, and the intent to establish legal relations, are utilized in electronic agreements. The study examines the legal acknowledgment of electronic records and digital signatures, emphasizing their significance in maintaining authenticity, integrity, and security in online dealings. Judicial rulings on click-wrap, browse-wrap, and shrink-wrap agreements are examined to grasp the changing stance of Indian courts regarding electronic contract practices. The research also tackles significant issues related to electronic contracts, such as cyber fraud, identity theft, data privacy worries, jurisdictional complexities, evidential challenges, and consumer protection in digital transactions. Particular focus is placed on the challenges emerging from cross-border e-commerce and the acceptance of electronic evidence as per Indian law. Furthermore, the study examines the effects of emerging technologies like

[1] Assistant Professor at R N Patel Ipcowala School of Law and Justice, The Charutar Vidya Mandal (CVM) University (India). Email:prakashgm.pa@gmail.com

blockchain and smart contracts, which are expected to shape the future of digital agreements and business regulation.

II. KEYWORDS

Electronic contracts, Information Technology Act, digital signatures, e-commerce, electronic evidence.

III. INTRODUCTION

From paper to digital contracts, from physical to e-form, the digital revolution has fundamentally transformed commercial activities across India. With the increasing penetration of the internet, smartphones, electronic banking, online marketplaces, and digital payment systems, contractual relationships are increasingly conducted through electronic means. Traditional paper-based contracts are gradually being replaced by electronic contracts executed through websites, emails, mobile applications, and automated digital systems.

Electronic contracts have become indispensable in sectors such as:

1. E-commerce,
2. Banking,
3. Insurance,
4. Information technology,
5. Telecommunications,
6. Online education,
7. Digital entertainment

The COVID-19 pandemic has intensified the shift towards digital transactions and remote business functions in India, leading to a greater dependence on electronic contracting methods., There has been a significant shift in handling matters, whether financial or contractual in the post Covid-19. There is a change in the model from paper to electronic format.

Electronic contracts offer convenience and efficiency, but they also present significant legal and technological challenges. Some of the key challenges that emerged in the Indian scenario is about the concerns over the validity of online contracts, party authentication, enforceability of digital transactions, cyber-security risks, and the admissibility of electronic evidence in the cyber laws.

To overcome these challenges India has enacted the Information Technology Act, 2000, which has been amended from time to time to address the changing needs, validity of electronic records and digital signatures. Judiciaries have also played a crucial role in the understanding and application of electronic contracts through judicial interpretations.

This research paper examines the electronic contracts in India through three thematic dimensions:

1. Validity of electronic contracts,
2. Authentication mechanisms in digital transactions, and
3. Enforcement and legal challenges under Indian law.

A. Research Objectives

The objectives of this research paper are:

1. To analyze the legal validity of electronic contracts in India.
2. To examine authentication mechanisms such as electronic and digital signatures.
3. To study the enforceability of electronic contracts under Indian law.
4. To evaluate challenges associated with electronic contracting in India.
5. To suggest reforms for strengthening India's electronic contracting framework.

B. Research Questions

The present study seeks to answer the following research questions:

1. What is the legal validity of electronically formed contracts under Indian law, particularly under the Indian Contract Act, 1872 and the Information Technology Act, 2000?
2. How does authentication through electronic and digital signatures satisfy the legal and evidentiary requirements applicable to electronic contracts in India?
3. What procedural, evidentiary, and jurisdictional challenges impede the enforcement of electronic contracts in India?

C. Research Methodology

Sr. no	Components	Description
1	Type of research design	Descriptive research design
2	Method of study	Statutory Reports, Judicial Precedents, judgments, legal commentaries
3	Sample size	Purposive sampling
4	Statistical technique	Qualitative technique
5	Data source	Statutory Reports, Judicial Precedents, judgments, legal commentaries

IV. CONCEPT OF ELECTRONIC CONTRACTS

E-contract, or electronic contract, is an agreement formed and carried out via digital technology and electronic communication. These agreements are frequently utilized in e-commerce, online banking, software licensing, mobile apps, and various other digital exchanges. Rather than signing hard copies, individuals form agreements through electronic means like emails, e-signatures, or online consent buttons. The rise of information technology and e-commerce has greatly boosted the utilization of electronic

contracts in contemporary business practices. Electronic contracts offer a fast and easy way to carry out transactions without needing the physical presence of those involved. They are commonly utilized by companies, consumers, and government bodies for effective communication and business transactions.

In India, electronic contracts are acknowledged legally under the Information Technology Act, 2000 in consonance with the provisions enumerated in the Indian Contract Act, 1872. Section 10A of the Information Technology Act affirms that a contract created electronically cannot be invalidated solely due to its digital existence.

The fundamental components of a valid enforcing contract according to the Indian Contract Act, 1872 still apply to electronic contracts, which interalia includes:

1. Offer
2. Acceptance
3. Lawful consideration
4. Free consent
5. Competency of parties
6. Lawful object.

Based on the above components' electronic contracts/ e-contracts can be made through:

1. Emails
2. Websites
3. Mobile applications
4. Electronic Data Interchange (EDI)
5. Online platforms.

Thus e-contracts differ only in the mode of communication and execution.

V. PART-I: VALIDITY OF ELECTRONIC CONTRACTS IN INDIA

A. Legal Framework Governing Electronic Contracts in India

Electronic Contracts are governed by the following legislations:

1. Indian Contract Act, 1872

The fundamental legislation for all types of contracts is The Indian Contract Act-1872. The legislation establishes the fundamental principles regulating contracts in India. Even though it was implemented long before the digital age, its stipulations are relevant to electronic agreements as well.

In order to be valid electronic contract to be valid, the following conditions must be met:

- A lawful offer and acceptance,
- Must have free consent,
- The agreement must not be void or unlawful.

The Indian Contract Act does not specify a required physical format for most contracts, thus permitting electronic agreements.

Recently, the manner in which e-contracts are formed has evolved. When business entities negotiate by exchanging documents that include their own pre-written terms and conditions, the scenario is commonly termed a "battle of forms."

Illustration: Let's consider a scenario involving a sale of goods transaction. In this scenario, a purchaser might ask the vendor to deliver certain goods, after which the vendor presents an offer based on its usual contractual conditions. Once the parties agree on the core commercial elements of the agreement like the type, amount of goods, pricing, delivery schedules, and inspection criteria, the buyer issues a purchase order that includes its own standard terms and conditions. The seller can subsequently confirm or recognize the order. In modern business operations, these communications and contractual exchanges are often carried out via email correspondence than the physical exchange of letters.

Under the Indian Contract Act, 1872, a valid contract is formed through a lawful proposal and its absolute and unqualified acceptance. Section 7 of the Act expressly provides that acceptance must be absolute and unqualified in order to convert a proposal into a promise. The Supreme Court in Bhagwandas Goverdhandas Kedia v. Girdharilal

Parshottamdas & Co. emphasized that a binding contract comes into existence when valid acceptance is communicated in accordance with law. Similarly, in Haridwar Singh v. Bagun Sumbrui, the Supreme Court reiterated that acceptance must correspond with the terms of the offer and be free from qualifications or variations. Therefore, an unqualified acceptance signifies complete assent to the terms of the offer and results in the formation of a legally enforceable contract.

2. Information Technology Act, 2000

The primary law regulating electronic transactions in India is the Information Technology Act, 2000. The legislation is enacted on the UNCITRAL Model Law (United Nations Commission on International Trade Law) established by the United Nations. As we are the signatory party of the UN, we formed this law to meet the global requirement.

- **Legal Recognition of Electronic Records:** Section 4 of the Information Technology Act 2000 grants legal acknowledgment to electronic records. This indicates that information cannot be dismissed as having no legal effect simply due to its existence in electronic format. To attract the provision of it, one must meet two conditions in this section:
  - **Electronic availability:** it must be rendered or made available in an electronic form
  - **Accessibility and usability:** it must be accessible so that it can be used subsequently
- **Legal Recognition of Digital Signatures:** Section 5 of the information technology act recognizes digital signatures as legally valid authentication methods. Digital signatures authenticate electronic records through cryptographic systems.
- **Validity of Electronic Contracts:** Section 10A of the IT Act explicitly recognizes contracts formed through electronic means. It states that contracts should not be deemed unenforceable solely because:
  - Electronic communication was used,

- Electronic records were involved.

This provision forms the legal foundation for e-commerce transactions in India.

B. Various types of Electronic Contracts in India

E-contracts, also referred to as electronic contracts, are agreements created and finalized via electronic methods including websites, emails, mobile apps, and digital platforms. Due to the swift expansion of e-commerce and online services, electronic contracts have emerged as a vital component of contemporary commercial dealings in India. These agreements are legally acknowledged according to the Information Technology Act of 2000 and the Indian Contract Act of 1872.Various types of electronic agreements are utilized based on the type of transaction and the way acceptance occurs. The primary categories of electronic contracts in India include:

1. **Click-Wrap Agreements:** These agreements require users to click an "I Agree" button before accessing services. A few common examples like:
   - Software licenses,
   - Mobile applications,
   - E-commerce websites.

   Indian courts generally recognize click-wrap agreements because they involve express consent.
2. **Browse-Wrap Agreements:** Browse-wrap agreements rely upon implied consent through website usage. These agreements are more controversial because:
   - Users may not read terms,
   - Consent may not be explicit.
3. **Shrink-Wrap Agreements:** Shrink-wrap agreements are commonly used in software products where contractual terms become binding upon opening the package or using the software.
4. **Electronic Banking and Fintech Contracts:** Digital payment platforms such as:

- Internet banking,
- Unified Payments Interface (UPI),
- Mobile wallets,

Fintech platforms (commonly used by the banks and financial sectors) rely heavily upon electronic contracts and digital consent mechanisms.

C. Judicial Recognition of Electronic Contracts in India- (case studies)

Indian courts have increasingly recognized electronic contracts and electronic evidence.

1. Case Study- I Trimex International FZE Ltd. v. Vedanta Aluminium Ltd.

The Supreme Court determined that a valid and enforceable agreement had been formed between the parties via the exchange of e-mails. The Court noted that when parties consent to the key terms of a contract, a lack of a formal signed document does not nullify the contract. The Court also determined that an arbitration agreement may be inferred from electronic communications and exchanges between parties if their intent to resolve disputes through arbitration is evident.

The Court emphasized that:

- Modern commercial transactions are often conducted electronically.
- E-mails and electronic records are legally recognized forms of communication.
- A concluded contract does not always require a signed document if offer and acceptance are clearly established.

This case confirmed that formal signed documents are not always necessary for contract formation.

2. Case study- II State of Maharashtra v. Dr. Praful B. Desai

In this instance, the Court highlighted that laws should evolve in response to technological progress and shifting societal circumstances. It noted that contemporary technology ought to be utilized to guarantee efficient justice administration and prevent

unwarranted delays in legal proceedings. The Supreme Court acknowledged the legitimacy of electronic communication and video conferencing in court proceedings. This case reinforced the acceptance of digital procedures in Indian law.

3. Case Study- III Shafhi Mohammad v. State of Himachal Pradesh

In this case, the Supreme Court determined that the mandate for a certificate under Section 65B (4) is procedural and may be waived when the individual presenting the electronic evidence lacks possession or control of the original device. The Court noted that requiring a certificate in each instance could lead to unfairness, particularly when the device is managed by a different party. Consequently, electronic evidence may still be allowed if its legitimacy is otherwise confirmed. The Court examined the admissibility of electronic evidence under the framework that was then contained in Sections 65A and 65B of the Indian Evidence Act, 1872, provisions that are now substantially reflected in Sections 62 and 63 of the Bharatiya Sakshya Adhiniyam, 2023.

The major observations of the court are as follows:

- Electronic evidence is an important part of modern legal proceedings.
- Procedural requirements should not defeat the cause of justice.
- Videography helps ensure fairness, transparency, and accuracy in investigations.
- Technology should be actively adopted in judicial and investigative processes.

4. Case Study- IV Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal

A significant question before the Court was whether electronic records could be admitted without compliance with Section 65B(4) of the Indian Evidence Act, 1872, a provision now substantially replicated in Section 63(4) of the Bharatiya Sakshya Adhiniyam, 2023.The Supreme Court ruled that the certificate requirement specified in Section 65B(4) is essential for admitting electronic evidence when it is offered as secondary electronic

records. The Court upheld the previous ruling in Anvar P.V. v. P.K. Basheer and rejected the opposing perspective from Shafhi Mohammad v. State of Himachal Pradesh.

The Court clarified that:

- Electronic evidence such as CDs, VCDs, CCTV footage, and computer outputs can be admitted only if accompanied by a proper Section 65B certificate.
- If the original electronic device itself is produced before the court, the certificate may not be necessary.
- Courts may permit parties to obtain the certificate at a later stage if it was not initially available.

5. **Case V- Goqii Technologies Private Limited v. Sokrati Technologies Private Limited.**

In this case, the dispute arose from a Master Services Agreement relating to digital marketing services that contained an arbitration clause. The principal issue before the Supreme Court was whether, at the stage of appointing an arbitrator under Section 11 of the Arbitration and Conciliation Act, 1996, the Court should undertake a detailed examination of the merits of the dispute or restrict itself to determining the prima facie existence of a valid arbitration agreement.

The Supreme Court held that the scope of inquiry under Section 11 is limited and that courts should ordinarily confine themselves to examining whether a valid arbitration agreement exists between the parties. Questions relating to the merits of the dispute are generally to be determined by the arbitral tribunal in accordance with the principle of kompetenz-kompetenz.

The Court observed that:

Judicial intervention at the pre-arbitration stage should remain minimal.

- The existence of a valid arbitration agreement is the primary consideration under Section 11 of the Arbitration and Conciliation Act, 1996.

- Commercial agreements executed through digital means are capable of containing valid and enforceable arbitration clauses.
- Issues relating to contractual performance and substantive disputes should ordinarily be decided by the arbitral tribunal.

This decision reinforces the judicial policy favouring arbitration and highlights the enforceability of arbitration agreements incorporated in electronically executed commercial contracts.

VI. PART-II: AUTHENTICATION OF ELECTRONIC CONTRACTS IN INDIA

A. Importance of Authentication

Timeline of how the authentication level came

Time	Description
1990	The rise of the internet and web applications led to the development of Single Sign-On
2000	Advances in sensor technology and computing power made the use of biometric data a real thing, not just something we see in movies
2010	This was the decade when MFA and token-based authentication became more widespread
2020	Driven by the need to reduce password-related vulnerabilities, password-less authentication methods gain traction

Authentication involves verifying the identity of a user or system prior to granting access. It functions by verifying credentials, like passwords or security tokens, against data held in a protected database. This security protocol aids in blocking unauthorized individuals from reaching sensitive information and safeguarded assets.

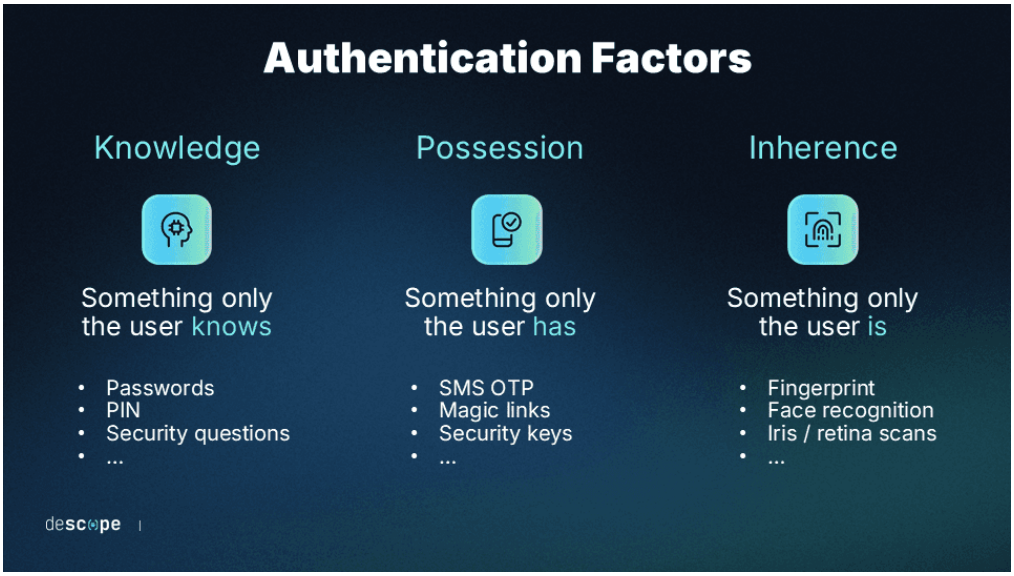
Single-factor authentication (SFA) depends on a single verification method, typically involving a username and password. Two-factor authentication (2FA) enhances security by necessitating an extra confirmation step, like a one-time code sent to a smartphone. Multifactor authentication (MFA) offers enhanced security by employing three or more verification approaches, which can consist of passwords, security tokens, and biometric identification such as fingerprints or facial recognition.

Authentication is essential for:

1. Verifying identity,
2. Ensuring integrity of records,
3. Preventing fraud,
4. Establishing non-repudiation.

Inadequate authentication can diminish the evidentiary value of electronic contracts.

Authentication and authorization fulfill distinct roles in security frameworks. Authentication serves to confirm a user's identity by addressing the inquiry, "Who are you?" Conversely, authorization specifies the extent of access or actions a confirmed user is allowed to take, addressing the query, "What can you do?"



B. Electronic Signatures and Digital Signatures

Section 2(1) (ta) defines about the electronic signature and says that “"electronic signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature.” Whereas Section 2(1)(p) says about the digital signature which means “the authentication of any electronic record by a person who has subscribed for the digital signature in accordance with the procedure mentioned under section 3 of the same act.”

1. **Electronic Signatures:** Electronic signatures include -
   - Typed names,
   - Electronic acceptance buttons,
   - Scanned signatures
   - Aadhaar-based authentication.

   They indicate contractual consent.

2. **Digital Signatures:** Digital signatures are more secure forms of authentication using asymmetric cryptography. The cryptography is involved in:
   - Public keys,
   - Private keys,
   - Hash functions,
   - Digital Certificates.

   The cryptographic integrity mechanism may be represented as:

   - H(m)=h
   - Where: m = electronic message
   - H(m) = hash value
   - h = digital fingerprint.

   Digital signatures provide three-layer features which are:

   - Authentication,

- Data integrity,
- Non-repudiation.

C. Difference between Electronics Signature and Digital Signature

Distinction	Electronic Signature	Digital Signature
Definition	Section 2(1) (ta)	Section 2(1)(p)
Working	It is technologically agnostic, meaning that no particular technological procedure needs to be used to establish an electronic signature.	It adopts a method dependent on the technology used, works thru hash functions.
Mode	It can be made with any technology which is currently used	It's made up of private key and public key using cryptographic and hash functions
Form	It can take the form of code, fingerprint, a name at the end of email	It's a two-way protection mechanism with a cryptographic technique for producing the signature
Trustworthy	Not much trust can be placed in an electronic signature	Higher level of trust can be placed in digital signature
Usage	To validate the document	To secure the document

Expiry period	No expiry period	Maximum of three years period
Tamper proof	Easy to be tampering	More secure hence not easily tampered

D. Certifying Authorities in India

In India, Certifying Authorities (CAs) are reliable entities sanctioned by the Information Technology Act, 2000 to provide Digital Signature Certificates (DSCs). These certificates serve as digital identity credentials that confirm the legitimacy of people, companies, and other organizations in online transactions. Through secure digital authentication, CAs support the confidentiality, integrity, and non-repudiation of online communications. Their services are commonly employed in e-governance, e-commerce, income tax submissions, business registrations, and various legally acknowledged electronic operations. The Certifying Authorities Controller (CCA) oversees these authorities in India.

The Functions of certifying authorities include:

- Verification,
- Issuance of digital certificates,
- Authentication management

E. Aadhaar-Based Authentication

Aadhaar authentication is a verification procedure where an individual's Aadhaar number, along with supporting details like demographic information, biometric data, or a one-time password (OTP), is sent to the Central Identities Data Repository (CIDR) of the Unique Identification Authority of India (UIDAI). The CIDR verifies if the provided details match the records in its database and then gives a straightforward "Yes" or "No" answer. Crucially, no personal identifying information is revealed throughout this procedure. The primary goal of Aadhaar authentication is to assist individuals in securely

proving their identity while allowing service providers to confirm the legitimacy of those requesting access to services, benefits, or subsidies. India has created distinctive digital identity systems via Aadhaar for verification purposes. E-signatures based on Aadhaar enable the subsequent functionalities:

- Remote authentication,
- Paperless transactions,
- Electronic governance.

However, challenges relating to privacy, data security, surveillance concerns, and the accessibility of digital authentication systems continue to attract legal and regulatory scrutiny.

F. Case VI- Pragya Prasun v. Union of India (2025)

In this case, the Supreme Court examined the accessibility of digital verification mechanisms, including Aadhaar-based authentication, e-KYC, and video-KYC procedures, for persons with disabilities. The petition was brought by acid-attack survivors and a visually impaired individual who faced difficulties in accessing essential financial and telecommunication services due to inaccessible digital verification requirements.

The Court held that digital accessibility forms an integral part of the right to life, dignity, and equal participation guaranteed under Article 21 of the Constitution. It emphasized that technological advancement must be accompanied by inclusive design and accessibility standards so that people with disabilities are not excluded from digital services.

The Court issued directions to regulatory authorities, including the Reserve Bank of India (RBI), the Securities and Exchange Board of India (SEBI), the Insurance Regulatory and Development Authority of India (IRDAI), and the Department of Telecommunications (DoT), to ensure that digital verification and authentication systems are accessible to persons with disabilities.

The case highlights the following principles:

- Digital accessibility is a fundamental rights concern.
- Authentication systems must be inclusive and non-discriminatory.
- Aadhaar-based and digital verification mechanisms should accommodate the needs of persons with disabilities.
- Regulatory frameworks must balance technological efficiency with accessibility and equal access to services.

G. Cyber-security Challenges in India

Cyber security has emerged as a significant issue in India because of the swift expansion of digital technology, online banking, e-governance, and internet utilization. With India's transition to a digital economy, cyber threats are rapidly escalating. People, companies, and government bodies encounter numerous cyber security issues that impact privacy, financial stability, and national security.

A major challenge is cybercrime, which encompasses hacking, phishing, identity theft, online fraud, and ransomware attacks. Cybercriminals frequently focus on banks, companies, and social media users to acquire sensitive data and funds. Numerous individuals in India remain uninformed about secure online habits, rendering them vulnerable targets for cyber-attacks. Electronic contracts are prone to:

- Hacking,
- Identity theft,
- Phishing,
- Data breaches,
- Cyber fraud

Cyber fraud involves unlawful actions conducted via computers, digital devices, or the internet aimed at tricking individuals or entities for financial profit or illicit access to private information. As online banking, e-commerce, and digital communication rapidly expand, cyber fraud has emerged as one of the major issues in today's digital age.

Cyber fraud manifests in various ways, such as phishing emails, identity theft, online banking scams, hacking, credit card schemes, counterfeit websites, and social media deception. In phishing schemes, deceivers pose as reputable entities to lure individuals into disclosing confidential data like passwords, banking information, or OTPs. In the same way, identity theft happens when offenders exploit someone else's private information for illegal activities. India has experienced a rise in cybercrime incidents attributed to swift digitization. Failures in cyber-security could endanger:

- Consent,
- Authentication,
- Integrity of electronic records.

Organizations must therefore implement robust cyber-security measures taking into consideration their requirements and size along with the nature of information they are handling.

VII. PART- III: ENFORCEMENT OF ELECTRONIC CONTRACTS IN INDIA

A. Enforceability of Electronic Contracts

The enforceability of electronic contracts pertains to the legal acknowledgment and obligatory essence of agreements created via electronic methods like emails, websites, mobile apps, and online platforms. As digital commerce and online transactions continue to expand, electronic contracts have become a crucial element of contemporary business and communication. An electronic contract, often referred to as an e-contract, is formed when individuals consent to terms and conditions via electronic communication instead of conventional paper-based approaches. These agreements can exist in different formats, such as click-wrap contracts, browse-wrap contracts, and agreements finalized with electronic signatures.

In India, the validity of electronic contracts is mainly regulated by the Parliament of India via the Information Technology Act, 2000, in consonance with the Indian Contract Act,

1872. The Information Technology Act provides legal acknowledgment to electronic records and digital signatures, guaranteeing that contracts created electronically are not considered invalid solely because they are in digital format. Electronic contracts are binding in India if:

- Essential contractual elements exist,
- Electronic consent is valid,
- Authentication mechanisms are reliable.

The burden of proof often depends upon:

- Electronic records,
- Metadata,
- Communication logs,
- Digital signatures.

B. Electronic Evidence under Indian Law

1. Bharatiya Sakshya Adhiniyam, 2023

Bharatiya Sakshya Adhiniyam recognizes electronic evidence.

The Bharatiya Sakshya Adhiniyam, 2023 (BSA), which came into force on 1 July 2024, governs the admissibility and evidentiary value of electronic records in India. The BSA has replaced the Indian Evidence Act, 1872 while substantially retaining the legal framework relating to electronic evidence.

Sections 62 and 63 of the BSA govern the admissibility of electronic records and electronic evidence. These provisions recognize information stored, recorded, copied, or generated through electronic devices as admissible evidence, subject to the fulfilment of prescribed statutory requirements. Electronic records may be admitted without production of the original record where the conditions prescribed under the BSA are satisfied.

The law mandates that the computer utilized for creating the electronic record must have been consistently employed for storing or processing information during routine

business or official operations. The details in the electronic record ought to have been inputted into the system during the normal progression of such activities. It is essential that the computer operates correctly during the relevant time frame, and any malfunction must not have impacted on the precision or dependability of the record.

Electronic evidence may include:

- Emails,
- Server logs,
- Digital documents,
- Audio-video records,
- Electronic databases.

Certificate Relating to Electronic Records under Section 63(4) of the Bharatiya Sakshya Adhiniyam, 2023.

Electronic records produced as secondary electronic evidence generally require a certificate under Section 63(4) of the Bharatiya Sakshya Adhiniyam, 2023. This provision substantially incorporates the evidentiary requirements that previously existed under Section 65B (4) of the Indian Evidence Act, 1872.

The certificate confirms:

- Authenticity of electronic records,
- Proper functioning of computer systems,
- Integrity of data.

The certificate must contain the following-

- Identification of the electronic record.
- Description of the manner in which it was produced.
- Details of the computer or communication device used.
- Confirmation that the device was functioning properly.

- Signatures of the person responsible for operating the device or managing the system, along with an expert were required.

This requirement plays a crucial role in enforcing electronic contracts.

2. Consumer Protection and E-Commerce

The Consumer Protection Act, 2019 has bolstered consumer confidence in online commerce by providing increased security in digital transactions. It encourages transparency, accountability, and ethical behavior among e-commerce companies while protecting consumers from deceptive practices and exploitation in the digital marketplace. India has enhanced consumer protection in digital transactions by:

- Consumer Protection Act, 2019.
- Consumer Protection (E-Commerce) Rules, 2020.

These laws require:

- Transparent disclosures,
- Fair trade practices,
- Consumer grievance mechanisms,
- Protection against unfair contract terms.
- Online platforms must provide clear contractual information to consumers.

C. Jurisdictional Issues in India

Electronic contracts present jurisdictional issues as parties can be located in various states or countries. One challenge encountered by every court regarding electronic contracts is determining the appropriate jurisdiction. The civil procedure code outlines how to determine jurisdiction, and the courts follow that guidance when making jurisdiction decisions.

Courts determine jurisdiction based on:

- Place of business,

- Cause of action,
- Location of servers,
- Terms of agreement.

Cross-border disputes remain difficult to resolve efficiently.

D. Smart Contracts and Block-chain in India

Block-chain technology and smart contracts are increasingly being used in financial technology, supply chain management, real estate transactions, trade documentation, and digital asset systems. Smart contracts are self-executing agreements in which contractual terms are embedded into computer code and automatically performed when predetermined conditions are satisfied. Their ability to reduce transaction costs, improve transparency, and automate performance has generated significant interest among businesses and regulators.

However, India currently does not have a dedicated statute specifically governing smart contracts or block-chain-based contractual arrangements. Consequently, issues relating to the legal recognition of automated execution, allocation of liability for coding errors, dispute resolution, jurisdiction, and regulatory oversight continue to create uncertainty.

E. Regulatory Developments relating to Digital Assets and Blockchain

India's regulatory approach towards crypto-assets and blockchain technology continues to evolve. While no comprehensive legislation governing private cryptocurrencies has yet been enacted, policy discussions surrounding the proposed Cryptocurrency and Regulation of Official Digital Currency Bill, 2021 have influenced ongoing regulatory debates. Regulatory authorities, including the Reserve Bank of India (RBI), the Ministry of Electronics and Information Technology (MeitY), and the Securities and Exchange Board of India (SEBI), have consistently emphasized the need for consumer protection, financial stability, anti-money laundering compliance, and technological innovation in the digital asset ecosystem.

F. Digital Rupee (e₹) and Smart Contract Implications

A significant development in India's digital finance landscape is the introduction of the Central Bank Digital Currency (CBDC), commonly known as the Digital Rupee or e₹, by the Reserve Bank of India. Pilot projects launched for both wholesale and retail use cases have demonstrated the potential of state-backed digital currency systems for secure and efficient digital payments. The Digital Rupee has particular relevance for electronic contracts because future CBDC-based ecosystems may incorporate programmable payment mechanisms and automated settlement functions resembling smart contract execution. Such developments may facilitate conditional payments, automated performance of contractual obligations, and enhanced transparency in commercial transactions.

Nevertheless, the absence of a dedicated legal framework governing smart contracts raises several unresolved questions relating to enforceability, liability for software defects, allocation of risk in automated transactions, and dispute resolution. As blockchain technology and CBDC-based payment systems continue to expand, legislative clarification and regulatory guidance will be necessary to ensure legal certainty and effective governance of digitally executed agreements.

VIII. CHALLENGES FACING ELECTRONIC CONTRACTS IN INDIA

A. Digital Literacy

Digital literacy is the capability to utilize digital technologies, computers, mobile devices, and the internet efficiently, responsibly, and securely. It encompasses the abilities needed to retrieve, comprehend, assess, generate, and disseminate information via digital platforms. In today's world, being digitally literate is crucial for education, jobs, communication, and societal involvement. Numerous people in India possess inadequate digital knowledge concerning:

- Online consent,
- Contractual obligations,

- Cyber-security risks.

B. Infrastructure Gaps

The following are the infrastructure gaps which are faced in the villages and towns of our country.

- Poor internet connectivity,
- Limited technological access,
- Lack of digital resources.

C. Cybercrime

Cybercrime denotes illegal actions carried out via computers, digital tools, networks, or the internet. It encompasses crimes where technology is utilized either as a means to carry out the offense or as the objective of the crime itself. The swift expansion of digital communication, internet banking, e-commerce, and social networking has turned cybercrime into a significant issue impacting individuals, companies, and governments across the globe. Cybercrimes manifest in various ways, including hacking, identity theft, online fraud, cyber-stalking, phishing, data breaches, ransomware attacks, distributing malware, and unauthorized entry into computer systems. Financial fraud via counterfeit websites, the exploitation of personal data, and social media scams rank among the most prevalent cybercrimes in today's society. The primary danger in the digital realm is cyber threat. India is experiencing an increase in occurrences of:

- Financial fraud,
- Identity theft,
- Online scams.

These problems erode trust in electronic transactions, as many people, especially the elderly, lack awareness of cybercrime and are not familiar with technology.

D. Privacy Concerns

Privacy remains one of the most significant concerns associated with electronic contracts and digital transactions. The collection, storage, and processing of personal data through online platforms create risks relating to:

- Unauthorized access,
- Data misuse,
- Surveillance and profiling.

To address these concerns, India has enacted the Digital Personal Data Protection Act, 2023 (DPDP Act), which establishes a comprehensive framework governing the processing of personal data. The legal framework has been further strengthened through the notification of the Digital Personal Data Protection Rules, 2025, which operationalise key provisions of the Act and introduce detailed compliance requirements for data fiduciaries. The Rules provide for consent management mechanisms, obligations relating to data retention and erasure, breach notification requirements, and the functioning of the Data Protection Board of India. While the implementation of the framework is being undertaken through a phased compliance mechanism, the DPDP Act and the DPDP Rules, 2025 represent a significant advancement in the protection of personal data and privacy within India's digital ecosystem. Nevertheless, challenges relating to effective enforcement, regulatory compliance, and balancing innovation with privacy protection continue to require attention.

IX. FINDINGS OF THE STUDY

Based on the analysis and case studies the study identifies the following findings:

1. India legally recognizes electronic contracts under the IT Act, 2000.
2. Digital signatures provide reliable authentication mechanisms.
3. Electronic evidence plays a crucial role in contract enforcement.
4. Cybersecurity threats significantly affect electronic commerce.
5. Consumer protection laws are increasingly adapting to digital transactions.

6. The growing adoption of blockchain technology, smart contracts, and Central Bank Digital Currency (CBDC) systems such as the Digital Rupee highlights the need for a dedicated legal and regulatory framework governing automated contractual performance, digital assets, and blockchain-based transactions.
7. The lack of detailed and specific legislation regulating electronic contracts and their execution results in legal ambiguity in online transactions
8. When a contract is digitally executed under duress, coercion, undue influence, deception, or unintended acceptance, there is frequently no efficient method to simply cancel or reverse the transaction within the digital contract framework.

X. RECOMMENDATIONS

The following measures are recommended:

1. Strengthening cyber-security infrastructure in India
2. Increasing digital literacy and consumer awareness
3. Simplifying electronic evidence procedures
4. Developing a comprehensive legal and regulatory framework governing blockchain technology, smart contracts, digital assets, and CBDC-enabled contractual transactions
5. Enhancing data protection and privacy safeguards
6. Improving cross-border dispute resolution mechanisms
7. Encouraging secure authentication technologies
8. More stringent measures should be taken against violations of data privacy
9. Enhancing the protection of electronic contracts through advanced security mechanisms
10. Providing simple and user-friendly access to grievance and redressal mechanisms instead of complicated technical procedures

© 2026. LawFoyer International Journal of Doctrinal Legal Research (ISSN: 2583-7753)

XI. CONCLUSION

Electronic contracts have become a vital component of India's digital economy. The Information Technology Act, 2000, along with the Indian Contract Act, 1872, establishes a robust legal structure acknowledging the legitimacy and enforceability of electronic contracts.

Technologies for authentication like digital signatures, Aadhaar-based e-signatures, and cryptographic systems have enhanced confidence in electronic transactions. Simultaneously, issues related to cyber-security, privacy, digital literacy, and jurisdiction persist in impacting the efficiency of electronic contracting in India.

As India moves towards a technology-focused economy, ongoing legal and technological updates will be essential to guarantee safe, effective, and fair online trade. Upcoming advancements in block-chain technology, artificial intelligence, and decentralized identity systems will continue to influence the progression of electronic contracts in India.

XII. BIBLIOGRAPHY

A. Books

1. Singh, Yatindra. Cyber Laws. Universal Law Publishing.
2. Reed, Chris. Internet Law. Cambridge University Press.
3. Avtar Singh. Law of Contract and Specific Relief. Eastern Book Company.
4. Justice T. Ravindran. Cyber Laws in India.

B. Journal Articles

1. "Electronic Contracts and Indian Cyber Law," Indian Journal of Law and Technology.
2. "Digital Signatures and E-Commerce in India," Journal of Cyber Law Studies.
3. "Smart Contracts and Blockchain Regulation in India," National Law School Review.

C. Statutes

1. Indian Contract Act, 1872
2. Information Technology Act, 2000
3. Indian Evidence Act, 1872
4. Consumer Protection Act, 2019
5. Consumer Protection (E-Commerce) Rules, 2020
6. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
7. Bharatiya Sakshya Adhiniyam 2023
8. Digital Personal Data Protection Act, 2023.
9. Digital Personal Data Protection Rules 2025 (Gazette Notification dated 13 November 2025, Ministry of Electronics and Information Technology).

D. Cases

1. Connaught Plaza Restaurants (P) Ltd. v. Niamat Kaur, 2013 SCC Online Del 2320 (Delhi High Court).
2. Bhagwandas Goverdhandas Kedia v. Girdharilal Parshottamdas & Co., AIR 1966 SC 543.
3. Haridwar Singh v. Bagun Sumbrui, AIR 1972 SC 1242.
4. Trimex International FZE Ltd. v. Vedanta Aluminium Ltd. (2010) 3 SCC 1
5. State of Maharashtra v. Dr. Praful B. Desai. (2003) 4 SCC 601
6. Shafhi Mohammad v. State of Himachal Pradesh. (2018) 5 SCC 311
7. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1
8. Goqii Technologies Private Limited v. Sokrati Technologies Private Limited, Civil Appeal No. 12234 of 2024, decided on 7 November 2024, 2024, INSC 853; [2024] 11 SCR 530.
9. Pragya Prasun v. Union of India (2025 INSC 599)

E. Websites

1. Ministry of Electronics and Information Technology, India

2. Controller of Certifying Authorities, India
3. India Code
4. Supreme Court of India
5. https://www.descope.com/learn/post/authentication-types