



FUTURE OF ONLINE CONTRACTS AND E-SIGNATURES

¹Dr.Mansi Singh,

¹Assistant Professor

¹CLS,

¹GIBS, Rohini, Delhi, India

Abstract : Due to the rapid development of technology, several sectors are experiencing a transition towards digitalization. Changes have also occurred in the domain of signatures and agreements. Online contracts and electronic signatures have revolutionised time-consuming, inefficient, and vulnerable paper-based processes. This paper discusses the growth, benefits, and potential issues of electronic signatures and online contracts in the future.

Electronic signatures and online contracts are already commonplace thanks to advancements in digital technology. The development of cloud computing, blockchain technology, and artificial intelligence has led to improved digital security, authentication, and verification methods. Smart contracts built on the blockchain may be used to automate and enforce contractual obligations, cutting out the middleman and speeding up the processing of complicated transactions.

There are several benefits to using electronic signatures and digital contracts. First, they save time and effort by doing away with paper records, human labour, and physical file cabinets. Digital contracts may be created, signed, and stored in a matter of minutes, allowing for quicker transaction closures and greater operational efficiency. With the use of e-signatures, businesses are able to eliminate geographical barriers and streamline their international trade operations by working together remotely.

Electronic signatures and digital contracts also boost safety and lawfulness. Modern encryption algorithms, multi-factor authentication, and audit trails all work together to ensure the security of digital contracts and keep their details hidden from prying eyes. They also give a detailed record of the signing process, which helps reduce conflicts and makes it easier to comply with regulations.

However, many problems must be fixed before electronic signatures and digital contracts can reach their full potential. The digital nature of these contracts necessitates revisions to legal systems to ensure their enforceability across jurisdictions. Due to privacy concerns, data protection, and cyber risks, rigorous security measures are essential to safeguard sensitive information and prevent unauthorised access or modification.

There will be a lot more online contracts and electronic signatures in the future. Incorporating state-of-the-art technologies like machine learning, biometrics, and the Internet of Things (IoT) will increase the efficiency and safety of digital transactions. Intelligent contract management solutions are able to automate the processes associated with the contract lifecycle, provide real-time data, and integrate seamlessly with other business applications.

IndexTerms: Online contracts, E-signature, Future, Information Technology, contracts.

OBJECTIVE

The purpose of this study is to explore and analyse the possible applications and validity of electronic signatures and online contracts within the context of current and future legal and technical frameworks. Researchers may learn more about the current state of online contracting and e-signatures, potential future advances, and existing issues. Examining the benefits, legal repercussions, and technological advancements connected with online contracts and e-signatures, this research intends to contribute to a full understanding of the potential effect of these tools on commerce, legal processes, and consumer experiences in the digital era.

INTRODUCTION

E-contracts, or electronic contracts, are gradually replacing paper contracts as India becomes a fully digital nation. As technology has advanced, traditional methods of doing business have shifted, and remote workers are increasingly highly prized. Due to their low cost and many benefits, electronic contracts are gaining popularity among companies. Because of the significant restrictions on movement and physical contact brought on by the Covid-19 pandemic, it has also been difficult for people to physically congregate and sign new contracts. Companies have resorted to this strategy owing to the pressing needs of certain circumstances and the want to grow their businesses.¹

One should, and rightly so, "Embrace the transformative power of the digital age and step into a world where technology intertwines seamlessly with every aspect of our lives." The digital revolution has become so pervasive that it has started to govern the way contracts are made and carried out. The legislative framework of the nation is not a barrier to the rapid expansion of internet media to previously unreached parts of the world. The inclusion of new technology into legal frameworks has been called for in a number of court judgements since the late 1990s. From India's first online court case, which took place in the civil court on Bhadra in 2007¹, to India's first paperless court, which opened in Kerala in 2022¹, India's whole legal system has undergone profound change.

When it comes to cutting-edge technologies like electronic signatures and online contracts, the nation has witnessed a number of different case laws. Despite the court's frequent criticism and pointing out of their flaws, electronic agreements have frequently been recognised as valid. While it's true that "we tell the version of the story that makes us good," this unfortunately isn't the case during legal processes.

WHAT IS AN E-CONTRACT?

With the proliferation of the internet and the rise of electronic commerce, online contracts have grown in both importance and breadth. An online contract or electronic contract is one that is drafted, signed, and executed entirely digitally, most often through the internet. In theory, a digital contract is drafted in the same manner as a traditional paper one. If a sale is to be made through the Internet, the vendor desiring the sale must disclose product details, including description, price, and shipping costs, to the buyer. Interested buyers may show their agreement with the seller's terms and conditions by either giving it some thought, clicking the "I Agree" or "Click to Agree" button, or signing electronically. Multiple options exist for completing electronic signatures, including typing the signer's name into a signature box, pasting a scanned signature, or clicking a checkbox. After all terms have been met and the money has been paid, the deal may be sealed. Servers' primary function is to allow two computers to exchange data with one another. The idea behind the online contract is to facilitate the creation and use of commercial contract regulations for online company. Online Contract is a template for commercial transactions between customers and suppliers. Clickwrap contracts, shrink wrap contracts, and browse contracts are the three main categories of online agreements. Other forms of online contracts include those for employment, independent contractor work, consulting, resale, distribution, confidentiality, software creation, licencing, and escrow of source code. Despite our familiarity with these types of online contracts, few of us understand the technical and legal hurdles that must be overcome when actually putting one to use.

WHAT IS E-SIGNATURE?

An electronic signature, or "e-signature," is a digital representation of a person's handwritten signature, indicating that the signer agrees with the terms of a document or agreement. It serves as evidence that the person signing the agreement is who they claim to be and that they want to be legally bound by its contents. Electronic signatures are increasingly used in business and legal activities conducted entirely online.

E-signatures are created electronically, usually via the use of a computer programme or the internet. They provide many advantages over traditional handwritten signatures, including convenience, speed, and safety. To ensure the legitimacy and non-repudiation of signed documents, e-signature systems often use encryption techniques. This adds credibility and legal standing to the signature by making it more difficult to forge or alter.

Many jurisdictions have their own laws and regulations concerning the use of electronic signatures. In many jurisdictions, electronic signatures have the same legal weight as a handwritten signature. It's important to remember that certain documents need specific signatures, and that additional requirements may apply for signatures to be accepted in some domains or circumstances.

Signing papers electronically saves time, eliminates the need for paper documents, and paves the door for further process digitalization in today's increasingly digital world.

TRENDS OF E-SIGNATURE IN FUTURE

As e-signatures gain widespread acceptance over the next decade, we may categorise the following advancements as essential enablers, driving e-Signature capabilities.

¹THOMAS J. SMEDINGHOFF, *Electronic Contracts and Digital Signatures* (July 16, 2023).

Accessible on a mobile device: As cellphones grow increasingly common, more and more businesspeople are turning to them for their day-to-day tasks. This shift has increased demand for cross-platform, mobile-friendly electronic signature services.

Thanks to mobile adaptability, users may put their signature on documents whenever and wherever they like. This convenience is especially helpful for remote workers who need to sign and distribute documents while away from the office. It may also lead to happier customers in the long run. By providing a simple and hassle-free registration process, businesses can boost their brand recognition and customer loyalty. It also helps the bottom line by decreasing the need for paper-based operations like printing, distributing, and storing information.

As our culture increasingly revolves on our mobile devices, we should expect to see the trend towards e-signature mobile compatibility persist. Companies who don't use this technology may struggle to keep up with the dynamic consumer market.²

Solutions hosted in the cloud To say that electronic signatures have had a profound impact on modern business would be an understatement. The long-term goal is to digitalize everything to the point where people aren't needed at all. The process has been streamlined with the emergence of cloud-based solutions, making it faster, more practical, and cheaper. Integration of electronic signatures into cloud-based solutions like document management systems, electronic signature platforms, contract management software, and workflow automation tools is growing in popularity as it reduces the need for paper-based processes, which can be inefficient and prone to mistakes.

Integrating electronic signatures into cloud-based systems has several advantages, including increased security and compliance controls. Access restriction, encrypted data storage, and other safety features are all available. Digital audit trails created by e-signatures make it straightforward to track out any revisions or anomalies in the signing process.

Electronic signatures in cloud-based systems have, without a doubt, boosted efficiency and productivity in business. In the past, completing a document may take days, but today it can be done in minutes. This not only reduces the time spent on these tasks, but also the cost of printing, scanning, signing, mailing, and storing the final product.

As society as a whole grows increasingly digital, the necessity for electronic signatures in cloud-based software is only expected to grow. This pattern is likely to persist as businesspeople continue to prioritise efficiency, effectiveness, and safety.

Collaborative skillsets: As the usage of electronic signatures in public and governmental processes grew, so did the need for a comprehensive cooperation platform. Collaborative e-signature systems allow for the simultaneous access and signing of documents by several users in different locations. This feature is especially useful for companies that employ workers in different locations or who work from home.

In addition, the platform provides a consolidated dashboard where users can see the status of each signature in real time, guaranteeing a smooth and efficient signing process. Better collaboration and communication amongst signatories, made possible by the capacity to exchange papers and annotate or comment on them, increases the accuracy and speed with which documents may be prepared.

In conclusion, the increasing emphasis on collaboration via the use of e-signatures is a remarkable development in the industry. Providing a secure, efficient, and collaborative means to sign papers, these platforms are quickly gaining appeal among businesses of all kinds.

Fourth, blockchain integration: e-signatures conducted using blockchain technology are a future trend. Blockchain technology has made electronic signatures more secure, transparent, and unalterable than ever before. It may reduce or eliminate the need for intermediaries, saving money and making the process more efficient. This will be particularly useful in industries like banking and real estate where trustworthiness of signatures is paramount.

The use of blockchain technology may also help with the fraud issue. By recording each signature and transaction on the blockchain, any fraudulent activity may be quickly uncovered and halted.

By creating a secure, transparent, and efficient digital transaction system, blockchain technology will increase the trustworthiness and reliability of e-signatures in the future business environment.

Although advances in technology and legislation are important enablers of e-signature adoption, demand from businesses and their users is the primary driver of advancement. Users now anticipate complete digital document execution, rather than just a signature at the conclusion of the process. In an effort to fully digitalize a process, specialists have developed end-to-end solutions.

All work on the document, from its inception to its final execution, takes place online, with no paper or ink involved. To this end, e-signature systems may be embedded inside preexisting digital infrastructure, such as cloud-based applications.

Another innovation that is gaining traction is the use of server-side signing. Users are given the ability to mediate their own identity processes via the usage of digital IDs. In this way, users may sign papers on services with the confidence that their identities have been validated. With server-side signature, a TSP like e-Mudhra generates and manages the signing keys on behalf of the signatory.

In the present digital world, a fully digital process with end-to-end digitization is not just a competitive advantage but a need.

²SANTOSH K PANDEY, KAVITA BHATIA, JAHNAVI BODHANKAR, e-Sign - An Online Digital Service: Evolving Trends & use Cases, International Journal of Engineering Research & Technology (IJERT), Vol. 9 Issue 01, January-2020.

Improved Adherence to Rules and Laws In addition to these technological advances, changes in legislation are also anticipated to affect the trajectory of e-signatures. As more nations recognise the legal legitimacy of electronic signatures, regulations are shifting to encourage their usage in more contexts. There will be greater uniformity in the law, and e-signatures will be recognised and upheld in more contexts. In the United States, remote online notarial services are permitted in more than 35 states. Multiple Australian states now permit the use of advanced remote electronic witnessing tools. E-signatures for usage in business processes at financial institutions are also gaining legitimacy.

New regulations will boost the use of witnessing services for agreements that are electronically signed, making it easier to sign legal documents without being in the same physical spot. This shift is in reaction to the growing acceptance of remote work and the need that businesses stay operational during situations such as the COVID-19 pandemic. It will be more convenient for individuals and businesses alike to use trusted identities, and the security of the signing process will be assured.

VALIDITY OF E-SIGNATURES AND ONLINE CONTRACT

The country's well-developed legal framework for online contracts facilitates electronic commerce and digital transactions in India. Thanks to the Information Technology Act, the Indian Contract Act, and other laws, online contracts, data protection, consumer rights, and dispute resolution are all codified in law. In the ever-evolving world of online transactions, the purpose of the legal framework is to foster confidence, protect the interests of all parties, and provide clarity. Companies and individuals must satisfy certain legal requirements for their online contracts to be valid and enforceable.

VALIDITY OF ONLINE CONTRACTS: -

Conventional contracts, including verbal agreements created with the free consent of the contractual parties and for reasonable remuneration with legal purpose but not explicitly declared void, were accepted under the Indian Contract of 1872. Therefore, this Act contains no provision prohibiting the enforcement of electronic agreements if they have all the elements necessary for a valid contract.

It is generally accepted that the free and informed agreement of both parties is the foundation of every enforceable contract. Most electronic contracts are non-negotiable. A "take it or leave it" exchange always gives the user an option.

In many cases, particularly those involving renegotiation of contract terms, Indian courts have questioned the legitimacy of electronic contracts. Case law from the Supreme Court states that "in dotted line contracts there would be no necessity for a weaker party to negotiate as to presume to have equal negotiating strength." This was stated in the case of LIC India v. Consumer Education and Research Centre. The dotted line agreement specifies that he must take the service or return the goods. He could either accept the absurd terms and conditions or continue using the service forever.

VALIDITY OF E-SIGNATURES

Any need for a signature must be considered and deemed satisfied if the document is verified by an electronic signature in accordance with the regulations set out in Section 5 of the IT Act. Under Indian law, electronic/digital signatures and other authentic electronic signatures are legally binding in the same ways that handwritten signatures are. There is a presumption of validity for electronic documents signed using a valid electronic signature (as specified by the IT Act), which is considered to be equivalent to a wet signature.

Electronic signatures, or e-signatures, are legally binding and recognised wherever they are used. Many countries recognise and enforce the validity of electronic signatures if they meet certain criteria.

Many countries' laws and legislation explicitly acknowledge and manage electronic signatures. In the United States, for instance, e-signatures have a federal and state legal basis defined by the Uniform Electronic Transactions Act (UETA) and the Electronic Signatures in Global and National Commerce Act (ESIGN), respectively. A similar legal basis for e-signatures across EU member states is provided by the eIDAS Regulation adopted by the European Union. An electronic signature is only valid if it can be shown that the signer intended to sign the document in an electronic format. Examples of such actions include typing in one's name, selecting the "I agree" radio option, or using a digital signature service.

Electronic signatures and electronic transactions need the parties' mutual consent. One technique to prove agreement is by a specifically worded phrase in a contract or terms of service.

The identity of the signer must be verified to ensure that the e-signature is genuine and untampered with. Digital certificates, passwords, and biometric data are only some of the methods that may be used to confirm an individual's identity.

Electronic signatures provide an additional layer of security and authenticity for the signed document. Encryption and tamper-evident techniques are used to protect the authenticity of the signed document.

Keeping Accurate Records: When using an electronic signature, it is essential to record specifics such as the method used, the signatory's name, and the time and date the signature was created.

Some documents may be excluded from the rules regulating electronic signatures or may need additional steps. Wills, some family law documents, and other court files may be exceptions that prevent or limit the use of electronic signatures.

It's important to keep in mind that e-signatures may be governed by different laws depending on the country, state, or area. Because of this, you should consult local legislation and legal advice to find out whether electronic signatures are recognised and legally binding in your country.

LAWS GOVERNING ONLINE CONTRACTS

The Indian Contract Act of 1872³ is the law that applies to contracts in the country. Electronic contracts are governed by the Indian Contract Act in much the same way as traditional contracts are. An electronic contract must meet all of the requirements of the Act's provisions in order to be legally enforceable.

E-contracts are legally binding according to the Information Technology Act of 2000. Electronic signatures, also known as "e-signature" or "digital signature," are used to authenticate the legality of e-contracts in accordance with Section 3 of the Act. Section 4 of the IT Act, 2000 allows for valid acknowledgement of the electronic data when it is coupled with a hardcopy or printed structure and made accessible to the customer for future reference. Sections 65 through Section 71 of the IT Act⁴ detail the consequences for online wrongdoing inside India.

E-contracts are recognised by law in India under Section 10A of the Information Technology Act of 2000⁵. Thus, the IT Act excludes some types of electronic transactions from the definition of negotiable documents, including powers of attorney, trust deeds, wills, sales deeds, and conveyance deeds pertaining to real property.

According to Section 65 of the Indian Evidence Act, 1872⁶, the electronic documents used to make the contract must be accepted by the court. The Indian Evidence Act of 1872 was amended to include Sections 65A and 65B, which permit parties to prove the contents of electronic records in accordance with the Delhi High Court's acceptance of electronic contracts in *Societies Fes Products Nestle S.A & Anr v. Essar Industries & Ors.*

The case *State of Delhi v. Mohd. Afzal and Others*⁷ was heard by the Delhi High Court, which held that "electronic records are admissible as evidence." The Supreme Court of India ruled in the case *State of Punjab and Others v. Amritsar Beverages Ltd. and Others* that media in paper, optical, or magnetic formats may be admitted into evidence. Information included in an electronic record is admissible in court without the need for an original document, as per Section 65-B of the Indian Evidence Act⁸. To be admissible, evidence must conform to a variety of criteria laid forth in Section 65-B of the Evidence Act⁹.

LAWS GOVERNING E-SIGNATURES

According to the Indian Stamp Act of 1899¹⁰, some documents must be legibly stamped at the time of execution or sooner. There are currently no regulations in India that outline the process for digitally stamping documents. When stamps are acknowledged digitally, several states—including Maharashtra, Karnataka, and Delhi—explicitly include electronic documents in the need for stamping. Adobe Acrobat Sign is very adaptable and may be altered to serve such purposes.

Businesses should always consult with their internal legal team to determine whether a stamp is necessary before electronically signing and executing a document. If a document is signed, executed, and stamped digitally, the company should still produce a physical duplicate and have it stamped. Documents that have been incorrectly stamped may incur fines.

To submit any form, application, or document to a government agency; to obtain any licence, permission, or approval from a government agency; and to receive or make a payment in a specific manner using electronic means are all examples of situations where electronic or digital signatures are permissible under the IT Act. The governing body may set rules for how electronic records and signatures are regarded for these purposes. Applications, financial statements, prospectuses, returns, declarations, memoranda, articles, details of charges, and other details or documents, as well as any notices, must be filed in a computer-readable electronic form in pdf, as required by Rule 7 of the Companies (Registration Offices and Fees) Rules, 2014¹¹. A digital signature is required to confirm an electronic form under Rule 8, as stated by the Central Board of Direct Taxes. This includes the e-TDS/e-TCS and other forms.

Click-wrap, certificates not issued by a CA, and other methods for generating electronic contracts are not explicitly recognised by the IT Act but may still be used. According to Section 10-A of the IT Act, a contract that was formed electronically is not invalid just because it was drawn out digitally. However, as such non-recognized electronic signatures do not have the same presumption of validity as acknowledged electronic signatures, the legality of electronic contracts signed using them may be challenged. The signer may be required to provide evidence of the following in such a case:

CASE LAWS ON VALIDITY OF ONLINE CONTRACTS

Numerous legal analyses of the validity and enforceability of internet contracts have been prompted by their profusion. While specific circumstances and judgements may vary depending on the decision-making body.

a number of precedents have addressed the legality of online contracts. *Vedanta Aluminium Ltd. v. Trimex International Fze*¹². It is a well-known case involving electronic signatures and online contracts in India. The matter was heard by the Delhi High Court in 2010 C.E.

³Indian Contract Act, 1872.

⁴Section 71, Information Technology Act, 2000.

⁵Section 10A, Information Technology Act, 2000.

⁶Section 65, Indian Evidence Act, 1872

⁷*State of Delhi v. Mohd. Afzal and Others*, 2003 VIIAD Delhi 1, 107 (2003) DLT 385, 2003 (71) DRJ 178, 2003 (3) JCC 1669.

⁸Section 65-B, Evidence Act, 1872.

⁹Section 65-B, Evidence Act, 1872.

¹⁰the Indian Stamp Act, 1899.

¹¹Rule 7, Companies (Registration Offices and Fees) Rules, 2014.

¹²*Trimex International Fze Limited v. Vedanta Aluminium Limited*, 2010 (1) SCALE 574.

In this instance, Vedanta Aluminium, an Indian company, and Trimex International, a United Arab Emirates-based company, had executed a contract online. The agreement included the delivery of bauxite. However, disagreements emerged regarding how the parties should execute the agreement. The court's primary concern was whether or not the online contract was enforceable under the law. Trimex International asserts that all parties involved in the transaction communicated solely via email. However, Vedanta Aluminium argued that no contract existed because the requisite conditions had not been satisfied.

The Delhi High Court agreed with Trimex International that an email agreement could comprise a legally binding contract. The court determined that the parties' email exchanges contained the essential elements of a contract: an offer, an acceptance, and consideration. The significance of the parties' willingness to be bound by the terms of the contract was emphasised, and in this instance, the parties' email communications demonstrated their intent to be held legally liable.

This ruling established an important precedent for the legality and enforcement of internet-based contracts in India. It acknowledged that electronic communications, such as emails, can constitute valid offers and acceptances and that such transactions are subject to the same legal requirements as traditional contracts.

In addition to the 2015 landmark case *Shreya Singhal v. Union of India*¹³, other precedents have been significant. In this decision, the Supreme Court invalidated Section 66A of the Information Technology Act of 2000¹⁴, which had been extensively criticised for its vague and overly broad provisions criminalising internet expression. In the context of online communications and exchanges, the ruling emphasised the need to protect fundamental rights, including the right to free expression. This decision has far-reaching effects on the regulation of online content and activity, including online contracts. In the case of *Shafhi Mohammad v. State of Himachal Pradesh* (2018)¹⁵, the Supreme Court of India ruled that digital documents, including electronic signatures, may be used as legal evidence, emphasising the significance of electronic contracts as evidence. The court upheld the arbitration clause in an online contract in the case *M/s. Sanjiv Prakashan v. Poonam Sharma* (2019). The court acknowledged the parties' agreement that internet-based contract disputes may be resolved through arbitration. In the 2018 case *Uber India Systems Pvt. Ltd. vs. Competition Commission of India*¹⁶, Uber was accused of exploiting its dominant position in the ride-hailing industry. The online agreement between Uber and its drivers was lawful, and the Competition Commission of India (CCI) was tasked with investigating the allegations.

It is possible that courts have ruled that internet-based contracts are unenforceable. In *S. Ramanathan v. State Bank of India* (2010)¹⁷, the court ruled that a contract allowing the bank to unilaterally modify the terms of an online banking service without the consumer's knowledge or consent was unjust and unreasonable. The court ruled that the clause was unenforceable and invalid. In *M/S Shriram EPC Limited v. Rioglass Solar SA* (2018)¹⁸, the court ruled that an email purchase order without a signed written agreement did not constitute a legally binding contract. The court emphasised the necessity of a formal written agreement to establish a legally binding contract.

The rule that a person cannot be held to an online contract if they lacked the mental capacity to comprehend and consent to the terms at the time the contract was signed has been challenged in other instances. Without the knowledge or consent of the customer, discretionary terms and conditions were implemented.

Although there have been significant judgements in India regarding internet contracts, there has been no precedent-setting case law that focuses primarily on internet contracts. Cases such as *Shreya Singhal v. Union of India*, which emphasise the preservation of fundamental rights in the online environment, have had an indirect effect on the legal framework governing internet transactions.

CONCLUSION AND WAY FORWARD

In a series of decisions, Indian courts have upheld the validity and enforceability of electronic contracts. The use of electronic contract execution has increased in India and is expected to continue doing so. COVID-19 mandates the use of electronic signatures when executing contracts. Simple to implement and legally binding, these ways of capital punishment are gaining popularity. However, extra ramifications, such as stamp duty, must be carefully considered by the parties. Notarizing electronic contracts is also crucial. In India, electronic notarization is still not recognised. As a result, the notarization of electronic contracts requires a legal framework from the proper authorities.

It is expected that the usage of online contracts and e-signature will go even further in the future as technology advances and electronic transactions become commonplace. Future developments for electronic signatures and digital contracts are discussed, and implications are drawn.

Online contracts and e-signatures are expected to become more popular as more and more businesses and individuals embrace digital processes in pursuit of efficiency, economy, and portability. E-signatures and other digital solutions have gained momentum as the COVID-19 pandemic has increased the demand for distant collaboration and contactless transactions.

¹³*Shreya Singhal v. Union of India*, AIR 2015 SC 1523; Writ Petition (Criminal) No. 167 OF 2012.

¹⁴Section 66A, Information Technology Act, 2000.

¹⁵*Shafhi Mohammad v. State of Himachal Pradesh*, (2018) SPECIAL LEAVE PETITION (CRL.) No.2302 of 2017.

¹⁶*Uber India Systems Pvt. Ltd. vs. Competition Commission of India* CIVIL APPEAL NO. 641 OF 2017.

¹⁷*S. Ramanathan v. State Bank of India*, (2010) C.S.No.930 of 2010.

¹⁸*M/S Shriram EPC Limited v. Rioglass Solar SA*, (2018) CIVIL APPEAL NO. 9515 of 2018.

As the number of electronic signatures used grows, so too will the need of taking extra precautions to prevent fraud and unauthorised access. Advances in biometrics, encryption technology, and blockchain-based solutions may help increase the trustworthiness of electronic signatures and digital contracts.

Continued work is being put towards fostering interoperability across various e-signature platforms and systems to allow for the seamless integration and exchange of electronic documents across many platforms and jurisdictions. To do this, norms and conventions will be crucial.

Regulation and Legal Frameworks: Governments and regulatory bodies will likely continue revising and upgrading laws and frameworks to accommodate the challenges and opportunities brought about by online contracts and e-signatures. Possible methods include elucidating legal requirements, promoting international consistency, and fixing emerging issues with data protection, privacy, and electronic evidence.

Developing technologies such as blockchain and artificial intelligence (AI) may be integrated with e-signatures in the near future. Blockchain technology has the potential to improve trust and immutability, while artificial intelligence (AI) might streamline the creation and evaluation of contracts.

In conclusion, the future of online contracts and e-signatures is bright due to increasing adoption, improved security measures, and evolving legal frameworks. As businesses and individuals adopt digital workflows, electronic signatures are expected to proliferate. Knowing the specific laws and procedures controlling e-signatures in each nation is vital for ensuring compliance and the enforceability of electronic contra

