Information Technology Act, 2000 (IT Act)

The **Information Technology Act, 2000,** also known as the **IT Act,** was passed by the Indian Parliament on **17th October 2000**. It provides the legal framework for **electronic transactions, digital communication, and cybercrimes** in India. This law was designed to promote e-governance, regulate online transactions, and protect against cybercrimes.

The IT Act was modeled after the **UNCITRAL Model Law on Electronic Commerce** 1996 (United Nations), which aimed to provide a framework for international electronic commerce and digital transactions.

सूचना प्रौद्योगिकी अधिनियम, 2000, जिसे आईटी अधिनियम के नाम से भी जाना जाता है, भारतीय संसद द्वारा 17 अक्टूबर 2000 को पारित किया गया था। यह भारत में इलेक्ट्रॉनिक लेनदेन, डिजिटल संचार और साइबर अपराधों के लिए कानूनी ढाँचा प्रदान करता है। इस कानून को ई-गवर्नेंस को बढ़ावा देने, ऑनलाइन लेनदेन को विनियमित करने और साइबर अपराधों से सुरक्षा प्रदान करने के लिए डिज़ाइन किया गया था।

Main Purpose of the IT Act

The **main goal** of the IT Act is to promote secure **digital transactions,** make **cybercrimes** easier to handle, and ensure **e-governance,** and individual use the internet safely.
The Act has **94 sections** and is divides into **13 chapters**. The last few sections focus on changes to India's older law, the **Indian Penal Code, 1860.**

आईटी अधिनियम का मुख्य उद्देश्य सुरक्षित डिजिटल लेनदेन को बढ़ावा देना, साइबर अपराधों से निपटना आसान बनाना, ई-गवर्नेंस सुनिश्चित करना और व्यक्तियों द्वारा इंटरनेट का सुरक्षित उपयोग सुनिश्चित करना है।
इस अधिनियम में 94 धाराएँ हैं और यह 13 अध्यायों में विभाजित है। अंतिम कुछ धाराएँ भारत के पुराने कानून, भारतीय दंड संहिता, 1860 में बदलावों पर केंद्रित हैं।

Features of the IT Act

1. Digital Signatures: The IT Act grants **legal recognition** to **electronic signatures**, ensuring that digital transactions and contracts are legally valid, much like traditional handwritten signatures.

2. Cybercrime Regulation: The Act defines and penalizes several cybercrimes, such as **hacking**, **identity theft**, **cyber terrorism**, and **cyber stalking**. It provides legal recourse for victims of cybercrimes.

3. Cyber Cafes: The IT Act defines a **cyber cafe** as any place where internet access is provided for a fee to the public. Although the relevance of cyber cafes has diminished in recent years, the Act still recognizes them in its provisions.

4. Overriding Provisions: The Act also makes it clear that its rules are above other laws, like the Copyright Act, 1957, meaning they don't interfere with the rights granted by other laws.

5. Regulation of Digital Media: With the Intermediary Guidelines and Digital Media Ethics Code rules of 2021, the IT Act introduced a framework to regulate social media platforms and digital news content, including measures for addressing objectionable content and user data privacy.

6.Legal Recognition:

The primary objective is to provide legal sanction to transactions conducted through e-commerce and other electronic means, replacing paper-based methods.

7. Electronic Data Interchange (EDI):

The Act recognizes transactions that occur through EDI, a structured method for business information exchange between companies.

8. Electronic Records:

It establishes the legal status of electronic records, ensuring they are admissible as evidence and that information is retained in a usable and accurate electronic form.

9. Facilitating Government Services:

The Act enables the electronic filing of documents with government agencies, making the delivery of government services more efficient.

10. Business Transactions:

It supports various forms of online business activities, including buying and selling goods, services, and information, and other internal and external business workflows.

1. डिजिटल हस्ताक्षर: आईटी अधिनियम इलेक्ट्रॉनिक हस्ताक्षरों को कानूनी मान्यता प्रदान करता है, जिससे यह सुनिश्चित होता है कि डिजिटल लेनदेन और अनुबंध पारंपरिक हस्तलिखित हस्ताक्षरों की तरह ही कानूनी रूप से मान्य हैं।

2. साइबर अपराध विनियमन: यह अधिनियम हैकिंग, पहचान की चोरी, साइबर आतंकवाद और साइबर स्टॉकिंग जैसे कई साइबर अपराधों को परिभाषित और दंडित करता है। यह साइबर अपराधों के पीड़ितों के लिए कानूनी उपाय प्रदान करता है।

3. साइबर कैफ़े: आईटी अधिनियम साइबर कैफ़े को किसी भी ऐसे स्थान के रूप में परिभाषित करता है जहाँ जनता को शुल्क लेकर इंटरनेट की सुविधा प्रदान की जाती है। हालाँकि हाल के वर्षों में साइबर कैफ़े की प्रासंगिकता कम हो गई है, फिर भी अधिनियम अपने प्रावधानों में उन्हें मान्यता देता है।

4. अधिभावी प्रावधान: अधिनियम यह भी स्पष्ट करता है कि इसके नियम कॉपीराइट अधिनियम, 1957 जैसे अन्य कानूनों से ऊपर हैं, अर्थात ये अन्य कानूनों द्वारा प्रदत्त अधिकारों में हस्तक्षेप नहीं करते हैं।

5. डिजिटल मीडिया का विनियमन: मध्यस्थ दिशानिर्देशों और 2021 के डिजिटल मीडिया आचार संहिता नियमों के साथ, आईटी अधिनियम ने सोशल मीडिया प्लेटफॉर्म और डिजिटल समाचार सामग्री को विनियमित करने के लिए एक रूपरेखा पेश की, जिसमें आपत्तिजनक सामग्री और उपयोगकर्ता डेटा गोपनीयता को संबोधित करने के उपाय शामिल हैं।

6. कानूनी मान्यता:
इसका प्राथमिक उद्देश्य कागज-आधारित तरीकों की जगह ई-कॉमर्स और अन्य इलेक्ट्रॉनिक माध्यमों से किए गए लेनदेन को कानूनी स्वीकृति प्रदान करना है।

7. इलेक्ट्रॉनिक डेटा इंटरचेंज (EDI):
यह अधिनियम EDI के माध्यम से होने वाले लेनदेन को मान्यता देता है, जो कंपनियों के बीच व्यावसायिक सूचना विनिमय के लिए एक संरचित विधि है।

8. इलेक्ट्रॉनिक रिकॉर्ड:
यह इलेक्ट्रॉनिक रिकॉर्ड की कानूनी स्थिति स्थापित करता है, यह सुनिश्चित करता है कि वे साक्ष्य के रूप में स्वीकार्य हैं और जानकारी को एक उपयोगी और सटीक इलेक्ट्रॉनिक रूप में रखा जाता है।

9. सरकारी सेवाओं को सुगम बनाना:
यह अधिनियम सरकारी एजेंसियों के साथ दस्तावेज़ों की इलेक्ट्रॉनिक फाइलिंग को सक्षम बनाता है, जिससे सरकारी सेवाओं का वितरण अधिक कुशल हो जाता है।
10. व्यावसायिक लेनदेन:
यह विभिन्न प्रकार की ऑनलाइन व्यावसायिक गतिविधियों का समर्थन करता है, जिसमें वस्तुओं, सेवाओं और सूचनाओं की खरीद-बिक्री और अन्य आंतरिक और बाहरी व्यावसायिक कार्यप्रवाह शामिल हैं।

Digital Signature

A digital signature is a cryptographic technique used to validate the authenticity and integrity of digital messages, documents, or software. It provides a way for the recipient to verify that the sender is who they claim to be and that the content has not been altered since it was signed.

Digital signatures and certificates are two key technologies that play an important role in ensuring the security and authenticity of online activities. They are essential for activities such as online banking, secure email communication, software distribution, and electronic document signing. By providing mechanisms for authentication, integrity, and non-repudiation, these technologies help protect against fraud, data breaches, and unauthorized access.

डिजिटल हस्ताक्षर एक क्रिप्टोग्राफ़िक तकनीक है जिसका उपयोग डिजिटल संदेशों, दस्तावेज़ों या सॉफ़्टवेयर की प्रामाणिकता और अखंडता को सत्यापित करने के लिए किया जाता है। यह प्राप्तकर्ता को यह सत्यापित करने का एक तरीका प्रदान करता है कि प्रेषक वही है जो वह होने का दावा करता है और हस्ताक्षर किए जाने के बाद से सामग्री में कोई बदलाव नहीं किया गया है।

डिजिटल हस्ताक्षर और प्रमाणपत्र दो प्रमुख तकनीकें हैं जो ऑनलाइन गतिविधियों की सुरक्षा और प्रामाणिकता सुनिश्चित करने में महत्वपूर्ण भूमिका निभाती हैं। ये ऑनलाइन बैंकिंग, सुरक्षित ईमेल संचार, सॉफ़्टवेयर वितरण और इलेक्ट्रॉनिक दस्तावेज़ हस्ताक्षर जैसी गतिविधियों के लिए आवश्यक हैं। प्रमाणीकरण, अखंडता और अस्वीकृति-विरोधी तंत्र प्रदान करके, ये तकनीकें धोखाधड़ी, डेटा उल्लंघनों और अनधिकृत पहुँच से बचाने में मदद करती हैं।

Key Aspects of Digital Signatures:

- **Authentication:**
  Digital signatures confirm the identity of the sender, ensuring the document comes from the claimed source.
- **Integrity:**
  They guarantee that the document hasn't been tampered with after signing, as any alteration would invalidate the signature.
- **Non-repudiation:**
  Digital signatures make it difficult for the sender to deny having signed the document, as the signature is linked to the private key.
- **Public Key Infrastructure (PKI):**
  Digital signatures are often based on PKI, which involves using a pair of keys: a private key for signing and a public key for verification.
- **Digital Signature Certificate (DSC):**
  A DSC is a digital credential that contains the signer's verified identity and is used to create a digital signature.
- **Use Cases:**
  Digital signatures are widely used for various purposes, including:
- **Legal and Financial Transactions:** Validating contracts, agreements, and financial documents.
- **Government Filings:** Submitting tax returns, e-procurement, and other government documents.
- **Software and Code Signing:** Ensuring the authenticity of software and preventing tampering.
- **Secure Email:** Authenticating the sender and ensuring the email's integrity.
- **Remote Access:** Securing access to networks and systems.

● प्रमाणीकरण:

डिजिटल हस्ताक्षर प्रेषक की पहचान की पुष्टि करते हैं और यह सुनिश्चित करते हैं कि दस्तावेज़ दावा किए गए स्रोत से ही आया है।

● अखंडता:

वे गारंटी देते हैं कि हस्ताक्षर करने के बाद दस्तावेज़ में कोई छेड़छाड़ नहीं की गई है, क्योंकि किसी भी प्रकार का परिवर्तन हस्ताक्षर को अमान्य कर देगा।

● अस्वीकृति:

डिजिटल हस्ताक्षर, प्रेषक के लिए दस्तावेज़ पर हस्ताक्षर करने से इनकार करना मुश्किल बना देते हैं, क्योंकि हस्ताक्षर निजी कुंजी से जुड़ा होता है।

● सार्वजनिक कुंजी अवसंरचना (PKI):

डिजिटल हस्ताक्षर अक्सर PKI पर आधारित होते हैं, जिसमें कुंजियों की एक जोड़ी का उपयोग शामिल होता है: हस्ताक्षर के लिए एक निजी कुंजी और सत्यापन के लिए एक सार्वजनिक कुंजी।

● डिजिटल हस्ताक्षर प्रमाणपत्र (DSC):

DSC एक डिजिटल क्रेडेंशियल है जिसमें हस्ताक्षरकर्ता की सत्यापित पहचान होती है और इसका उपयोग डिजिटल हस्ताक्षर बनाने के लिए किया जाता है।

● उपयोग के मामले:

डिजिटल हस्ताक्षरों का व्यापक रूप से विभिन्न उद्देश्यों के लिए उपयोग किया जाता है, जिनमें शामिल हैं:

● कानूनी और वित्तीय लेनदेन: अनुबंधों, समझौतों और वित्तीय दस्तावेजों का सत्यापन।

● सरकारी फाइलिंग: कर रिटर्न, ई-खरीद और अन्य सरकारी दस्तावेज जमा करना।

● सॉफ्टवेयर और कोड साइनिंग: सॉफ्टवेयर की प्रामाणिकता सुनिश्चित करना और छेड़छाड़ को रोकना।

● सुरक्षित ईमेल: प्रेषक को प्रमाणित करना और ईमेल की अखंडता सुनिश्चित करना।

● रिमोट एक्सेस: नेटवर्क और सिस्टम तक पहुँच को सुरक्षित करना।

Benefits of Digital Signatures

- **Legal documents and contracts:** Digital signatures are legally binding. This makes them ideal for any legal document that requires a signature authenticated by one or more parties and guarantees that the record has not been altered.
- **Sales contracts:** Digital signing of contracts and sales contracts authenticates the identity of the seller and the buyer, and both parties can be sure that the signatures are legally binding and that the terms of the agreement have not been changed.
- **Financial Documents:** Finance departments digitally sign invoices so customers can trust that the payment request is from the right seller, not from a attacker trying to trick the buyer into sending payments to a fraudulent account.

- **Health Data:** In the healthcare industry, privacy is paramount for both patient records and research data. Digital signatures ensure that this confidential information was not modified when it was transmitted between the consenting parties.

• कानूनी दस्तावेज़ और अनुबंध: डिजिटल हस्ताक्षर कानूनी रूप से बाध्यकारी होते हैं। यह उन्हें ऐसे किसी भी कानूनी दस्तावेज़ के लिए आदर्श बनाता है जिसके लिए एक या अधिक पक्षों द्वारा प्रमाणित हस्ताक्षर की आवश्यकता होती है और यह गारंटी देता है कि रिकॉर्ड में कोई बदलाव नहीं किया गया है।
• बिक्री अनुबंध: अनुबंधों और बिक्री अनुबंधों पर डिजिटल हस्ताक्षर विक्रेता और खरीदार की पहचान प्रमाणित करते हैं, और दोनों पक्ष निश्चिंत हो सकते हैं कि हस्ताक्षर कानूनी रूप से बाध्यकारी हैं और समझौते की शर्तों में कोई बदलाव नहीं किया गया है।
• वित्तीय दस्तावेज़: वित्त विभाग चालानों पर डिजिटल हस्ताक्षर करते हैं ताकि ग्राहक यह विश्वास कर सकें कि भुगतान अनुरोध सही विक्रेता से है, न कि किसी हमलावर से जो खरीदार को धोखा देकर किसी धोखाधड़ी वाले खाते में भुगतान भेजने की कोशिश कर रहा है।
• स्वास्थ्य डेटा: स्वास्थ्य सेवा उद्योग में, रोगी रिकॉर्ड और अनुसंधान डेटा, दोनों के लिए गोपनीयता सर्वोपरि है। डिजिटल हस्ताक्षर यह सुनिश्चित करते हैं कि सहमति देने वाले पक्षों के बीच प्रेषित होने पर इस गोपनीय जानकारी में कोई बदलाव नहीं किया गया हो।

Drawbacks of Digital Signature

- **Dependency on technology:** Because digital signatures rely on technology, they are susceptible to crimes, including hacking. As a result, businesses that use digital signatures must make sure their systems are safe and have the most recent security patches and upgrades installed.
- **Complexity:** Setting up and using digital signatures can be challenging, especially for those who are unfamiliar with the technology. This may result in blunders and errors that reduce the system's efficacy. The process of issuing digital signatures to senior citizens can occasionally be challenging.
- **Limited acceptance:** Digital signatures take time to replace manual ones since technology is not widely available in India, a developing nation.

• तकनीक पर निर्भरताचूँकि डिजिटल हस्ताक्षर तकनीक पर निर्भर करते हैं :, इसलिए वे हैकिंग सहित अपराधों के प्रति संवेदनशील होते हैं। परिणामस्वरूप, डिजिटल हस्ताक्षरों का उपयोग करने वाले व्यवसायों को यह सुनिश्चित करना होगा कि उनके सिस्टम सुरक्षित हों और उनमें नवीनतम सुरक्षा पैच और अपग्रेड इंस्टॉल हों।

• जटिलताडिजिटल हस्ताक्षरों को सेट अप करना और उनका उपयोग करना चुनौतीपूर्ण हो : सकता है, खासकर उन लोगों के लिए जो तकनीक से परिचित नहीं हैं। इसके परिणामस्वरूप ऐसी

गलतियाँ और त्रुटियाँ हो सकती हैं जो सिस्टम की प्रभावशीलता को कम कर देती हैं। वरिष्ठ नागरिकों को डिजिटल हस्ताक्षर जारी करने की प्रक्रिया कभीकभी चुनौतीपूर्ण हो सकती है।-

• सीमित स्वीकृति हडिजिटल हस्ताक्षरों को मैन्युअल हस्ताक्षरों की जग :लेने में समय लगता है क्योंकि विकासशील देश भारत में तकनीक व्यापक रूप से उपलब्ध नहीं है।

How it is created

Digital signatures are created using asymmetric cryptography, also known as public-key cryptography. The process involves generating a pair of cryptographic keys: a private key and a public key. The private key is kept secret and known only to the signer, while the public key is shared with others. The digital signature is created by applying a mathematical algorithm to the content being signed and the signer's private key.

डिजिटल हस्ताक्षर असममित क्रिप्टोग्राफी का उपयोग करके बनाए जाते हैं, जिसे सार्वजनिक-कुंजी क्रिप्टोग्राफी भी कहा जाता है। इस प्रक्रिया में क्रिप्टोग्राफ़िक कुंजियों की एक जोड़ी उत्पन्न करना शामिल है: एक निजी कुंजी और एक सार्वजनिक कुंजी। निजी कुंजी गुप्त रखी जाती है और केवल हस्ताक्षरकर्ता को ही ज्ञात होती है, जबकि सार्वजनिक कुंजी दूसरों के साथ साझा की जाती है। डिजिटल हस्ताक्षर हस्ताक्षरित सामग्री और हस्ताक्षरकर्ता की निजी कुंजी पर एक गणितीय एल्गोरिथ्म लागू करके बनाया जाता है।

How it works

When a digital signature is created, it is attached to the digital document or message. To verify the signature, the recipient uses the signer's public key to decrypt the signature and compare it to a computed value based on the original content. If the two values matches, the signature is considered valid, indicating that the document has not been altered and was indeed signed by the holder of the private key.

डिजिटल हस्ताक्षर बनाते समय, उसे डिजिटल दस्तावेज़ या संदेश से जोड़ दिया जाता है। हस्ताक्षर की पुष्टि के लिए, प्राप्तकर्ता हस्ताक्षरकर्ता की सार्वजनिक कुंजी का उपयोग करके हस्ताक्षर को डिक्रिप्ट करता है और मूल सामग्री पर आधारित एक परिकलित मान से उसकी तुलना करता है। यदि दोनों मान मेल खाते हैं, तो हस्ताक्षर को वैध माना जाता है, जो दर्शाता है कि दस्तावेज़ में कोई बदलाव नहीं किया गया है और वास्तव में निजी कुंजी धारक द्वारा हस्ताक्षरित है।

E-Governance

Electronic Governance or E-Governance is the application of Information and Communication Technology (ICT) for providing government services, interchange of statistics, communication proceedings, and integration of various independent systems and services. Through the means of e-governance, government services are made available to citizens in a suitable, systematic, and transparent mode. The three main selected groups that can be discriminated against in governance concepts are government, common people, and business groups.
E-governance is the best utilization of information and communication technologies to mutate and upgrade the coherence, productivity, efficacy, transparency, and liability of informational and transnational interchanges within government, between government agencies at different levels, citizens & businesses. It also gives authorization to citizens through access and use of information. Generally, E-governance uses information and communication technologies at various levels of the government and the public sector to enhance governance.

Theoretical studies state that E-Governance is the procedure of change of the correlation of government with its ingredients, the citizens, the businesses, and its own organs, through the use of tools of information and communication technology.

The UNESCO states that E-governance is the public sector's use of information and communication automation in order to upgrade information and service delivery, stimulating resident involvement in the decision-making process and making government more liable, unambiguous and productive.

इलेक्ट्रॉनिक गवर्नेंस या ई-गवर्नेंस, सरकारी सेवाएँ प्रदान करने, आँकड़ों के आदान-प्रदान, संचार प्रक्रियाओं और विभिन्न स्वतंत्र प्रणालियों व सेवाओं के एकीकरण हेतु सूचना एवं संचार प्रौद्योगिकी (आईसीटी) का अनुप्रयोग है। ई-गवर्नेंस के माध्यम से, सरकारी सेवाएँ नागरिकों को उपयुक्त, व्यवस्थित और पारदर्शी तरीके से उपलब्ध कराई जाती हैं। शासन की अवधारणाओं में जिन तीन मुख्य समूहों के बीच विभेद किया जा सकता है, वे हैं सरकार, आम लोग और व्यावसायिक समूह।

ई-गवर्नेंस, सरकार के भीतर, विभिन्न सरकारी एजेंसियों के बीच, सूचनात्मक और अंतरराष्ट्रीय आदान-प्रदान की सुसंगतता, उत्पादकता, प्रभावकारिता, पारदर्शिता और उत्तरदायित्व को परिवर्तित और उन्नत करने के लिए सूचना एवं संचार प्रौद्योगिकियों का सर्वोत्तम उपयोग है।

यह नागरिकों और व्यवसायों के बीच संबंधों को बेहतर बनाने के लिए सरकार और सार्वजनिक क्षेत्र के विभिन्न स्तरों पर सूचना और संचार तकनीकों का उपयोग करता है।

सैद्धांतिक अध्ययनों से पता चलता है कि ई-गवर्नेंस सूचना और संचार तकनीक के माध्यम से सरकार के अपने घटकों, नागरिकों, व्यवसायों और अपने स्वयं के अंगों के साथ संबंधों को बदलने की प्रक्रिया है।

यूनेस्को का कहना है कि ई-गवर्नेंस सूचना और सेवा वितरण को उन्नत करने, निर्णय लेने की प्रक्रिया में नागरिकों की भागीदारी को प्रोत्साहित करने और सरकार को अधिक उत्तरदायी, स्पष्ट और उत्पादक बनाने के लिए सार्वजनिक क्षेत्र द्वारा सूचना और संचार स्वचालन का उपयोग है।

Elements of E-Governance

Basic elements of e-governance are:

1. Government
2. Citizens
3. Investors/Businesses

Types of E-Governance

E-governance is of 4 types:

1. **Government-to-Citizen (G2C):** The Government-to-citizen mentions the government services that are acquired by the familiar people. Most of the government services come under G2C. Similarly, the primary aim of Government-to-citizen is to supply facilities to the citizens. It also helps ordinary people to minimize the time and cost to carry out a transaction. A citizen can retrieve the facilities anytime from anywhere. Similarly, spending the administrative fee online is also possible due to G2C. The facility of Government-to-Citizen allows the ordinary citizen to outclass time limitations. It also focuses on geographic land barriers.

सरकार-से-नागरिक (G2C): सरकार-से-नागरिक उन सरकारी सेवाओं को संदर्भित करता है जो परिचित लोगों द्वारा प्राप्त की जाती हैं। अधिकांश सरकारी सेवाएँ G2C के अंतर्गत आती हैं। इसी प्रकार, सरकार-से-नागरिक का प्राथमिक उद्देश्य नागरिकों को सुविधाएँ प्रदान करना है। यह आम लोगों को लेन-देन में लगने वाले समय और लागत को कम करने में भी मदद करता है। एक नागरिक कभी भी, कहीं से भी सुविधाएँ प्राप्त कर सकता है। इसी प्रकार, G2C के कारण प्रशासनिक शुल्क का भुगतान भी ऑनलाइन संभव है। सरकार-से-नागरिक सुविधा आम नागरिकों को समय की सीमाओं से आगे निकलने में मदद करती है। यह भौगोलिक भूमि बाधाओं पर भी ध्यान केंद्रित करती है।

2. **Government-to-business (G2B):** Government-to-business is the interchange of services between Government and Business firms. It is productive for both government and business firms. G2B provides access to pertinent forms needed to observe. It also contains many services interchanged between business sectors and government. Similarly, Government-to-business provides timely business information. A business organization can have easy and easy online access to government agencies. G2B plays an important role in business development. It upgrades the efficiency and quality of communication and transparency of government projects.

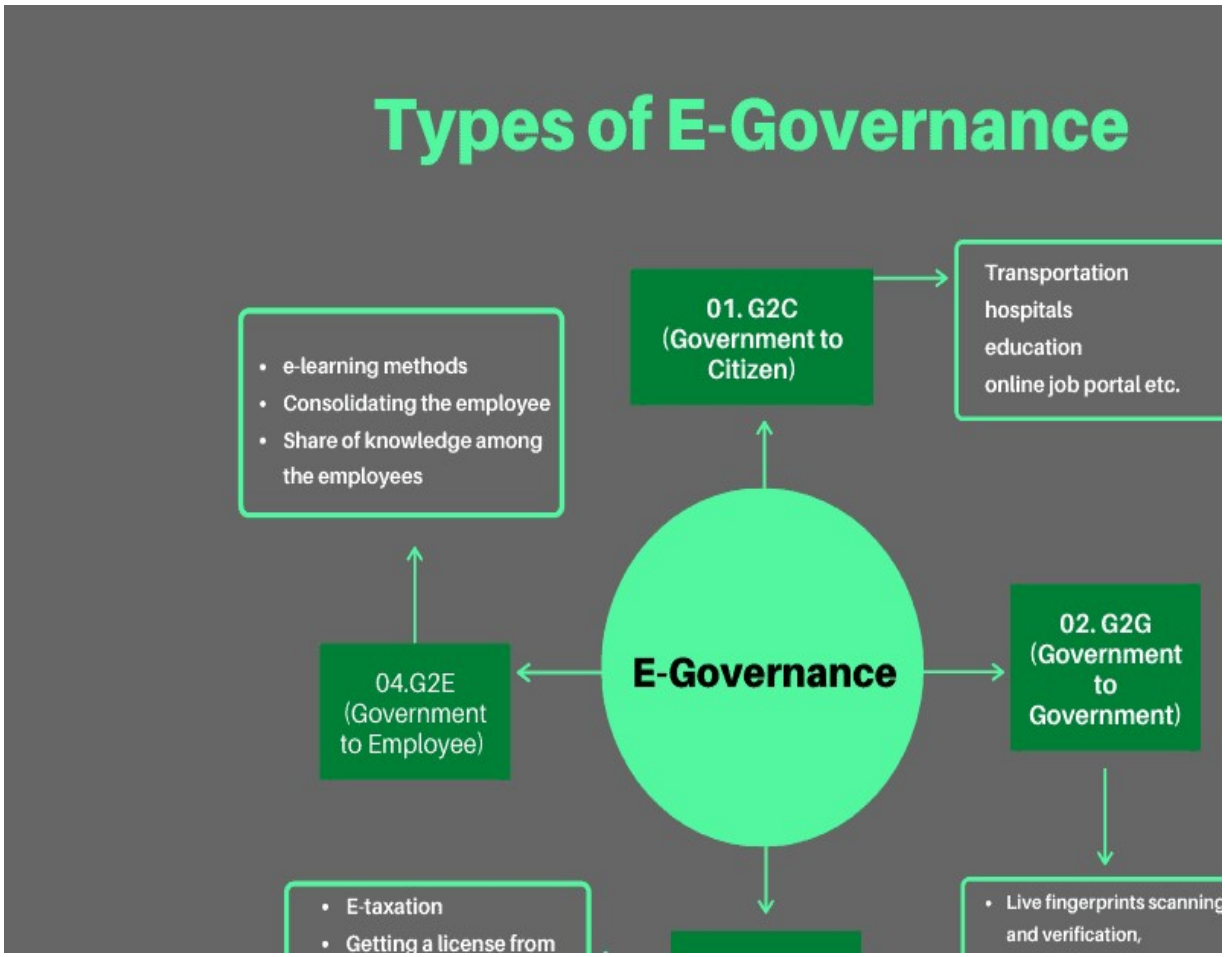
सरकार-से-व्यवसाय (G2B): सरकार-से-व्यवसाय, सरकार और व्यावसायिक फर्मों के बीच सेवाओं का आदान-प्रदान है। यह सरकार और व्यावसायिक फर्मों, दोनों के लिए लाभदायक है। G2B, निरीक्षण के लिए आवश्यक प्रासंगिक प्रपत्रों तक पहुँच प्रदान करता है। इसमें व्यावसायिक क्षेत्रों और सरकार के बीच आदान-प्रदान की जाने वाली कई सेवाएँ भी शामिल हैं। इसी प्रकार, सरकार-से-व्यवसाय, समय पर व्यावसायिक जानकारी प्रदान करता है। एक व्यावसायिक संगठन सरकारी एजेंसियों तक आसान और सरल ऑनलाइन पहुँच प्राप्त कर सकता है। G2B, व्यावसायिक विकास में महत्वपूर्ण भूमिका निभाता है। यह सरकारी परियोजनाओं की संचार दक्षता, गुणवत्ता और पारदर्शिता को बढ़ाता है।

3. **Government-to-Government (G2G):** The Government-to-Government mentions the interaction between different government departments, firms, and agencies. This increases the efficiency of government processes. In G2G, government agencies can share the same database using online communication. The government departments can work together. This service can increase international discretion and relations. G2G services can be at the local level or at the international level. It can convey to both global government and local government. It also provides a safe and secure inter-relationship between domestic and foreign governments. G2G builds a universal database for all members to upgrade service.

सरकार-से-सरकार (G2G): सरकार-से-सरकार विभिन्न सरकारी विभागों, फर्मों और एजेंसियों के बीच बातचीत को संदर्भित करती है। इससे सरकारी प्रक्रियाओं की दक्षता बढ़ती है। G2G में, सरकारी एजेंसियाँ ऑनलाइन संचार के माध्यम से एक ही डेटाबेस साझा कर सकती हैं। सरकारी विभाग एक साथ काम कर सकते हैं। यह सेवा अंतर्राष्ट्रीय विवेक और संबंधों को बढ़ा सकती है। G2G सेवाएँ स्थानीय या अंतर्राष्ट्रीय स्तर पर हो सकती हैं। यह वैश्विक सरकार और स्थानीय सरकार, दोनों को प्रदान की जा सकती हैं। यह घरेलू और विदेशी सरकारों के बीच एक सुरक्षित और विश्वसनीय अंतर्संबंध भी प्रदान करती है। G2G सभी सदस्यों के लिए सेवा उन्नयन हेतु एक सार्वभौमिक डेटाबेस बनाता है।

4. **Government-to-Employee (G2E):** The Government-to-Employee is the internal part of G2G section. It aims to bring employees together and improvise knowledge sharing. It provides online facilities to the employees. Similarly, applying for leave, reviewing salary payment record and checking the balance of holiday. The G2E sector yields human resource training and development. So, G2E is also the correlation between employees and government institutions.

सरकार-से-कर्मचारी (G2E): सरकार-से-कर्मचारी, G2G अनुभाग का आंतरिक भाग है। इसका उद्देश्य कर्मचारियों को एक साथ लाना और ज्ञान-साझाकरण में सुधार लाना है। यह कर्मचारियों को ऑनलाइन सुविधाएँ प्रदान करता है। इसी प्रकार, छुट्टी के लिए आवेदन करना, वेतन भुगतान रिकॉर्ड की समीक्षा करना और छुट्टियों के शेष की जाँच करना भी इसमें शामिल है। G2E क्षेत्र मानव संसाधन प्रशिक्षण और विकास प्रदान करता है। इसलिए, G2E कर्मचारियों और सरकारी संस्थानों के बीच संबंध भी है।



Advantages of E-Governance

The supreme goal of e-governance is to be able to provide an increased portfolio of public services to citizens in a systematic and cost effective way. It allows for government transparency because it allows the public to be informed about what the government is working on as well as the policies they are trying to implement.

The main advantage while executing electronic government will be to enhance the efficiency of the current system.

Another advantage is that it increases transparency in the administration, reduces costs, increases revenue growth, and also improves relationships between the public and the civic authorities.

ई-गवर्नेंस का सर्वोच्च लक्ष्य नागरिकों को व्यवस्थित और लागत-प्रभावी तरीके से सार्वजनिक सेवाओं का एक विस्तृत पोर्टफोलियो प्रदान करना है। यह सरकारी पारदर्शिता सुनिश्चित करता है क्योंकि इससे जनता को सरकार के कार्यों और उसके द्वारा लागू की जा रही नीतियों के बारे में जानकारी मिलती है।

इलेक्ट्रॉनिक शासन व्यवस्था का मुख्य लाभ मौजूदा व्यवस्था की दक्षता में वृद्धि करना होगा। एक अन्य लाभ यह है कि इससे प्रशासन में पारदर्शिता बढ़ती है, लागत कम होती है, राजस्व वृद्धि होती है और जनता और नागरिक अधिकारियों के बीच संबंध भी बेहतर होते हैं।

Disadvantages of E-Governance

The main disadvantage regarding e-governance is the absence of fairness in public access to the internet, of trustworthy information on the web, and disguised agendas of government groups that could have an impact and could bias public opinions.

ई-गवर्नेंस के संबंध में मुख्य नुकसान यह है कि इंटरनेट तक सार्वजनिक पहुंच में निष्पक्षता का अभाव है, वेब पर विश्वसनीय जानकारी नहीं है, तथा सरकारी समूहों के छिपे हुए एजेंडे हैं, जिनका प्रभाव पड़ सकता है तथा जनता की राय पक्षपातपूर्ण हो सकती है।

Attribution In Ecommerce

Ecommerce attribution is the process of assigning credit for a sale or conversion to the different marketing touchpoints a customer encountered along their journey, helping businesses understand which channels and campaigns are driving revenue and how to allocate their marketing budget most effectively. It answers the question of which marketing activities caused a customer to make a purchase by tracking interactions from initial awareness to final sale, using various attribution models to distribute credit across the customer journey.

ई-कॉमर्स एट्रिब्यूशन, किसी बिक्री या रूपांतरण का श्रेय ग्राहक द्वारा अपनी यात्रा के दौरान देखे गए विभिन्न मार्केटिंग टचपॉइंट्स को देने की प्रक्रिया है। इससे व्यवसायों को यह समझने में मदद मिलती है कि कौन से चैनल और अभियान राजस्व बढ़ा रहे हैं और अपने मार्केटिंग बजट को सबसे प्रभावी ढंग से कैसे आवंटित किया जाए। यह इस सवाल का जवाब देता है कि किन मार्केटिंग गतिविधियों के कारण ग्राहक ने खरीदारी की, शुरुआती जागरूकता से लेकर अंतिम बिक्री तक के इंटरैक्शन को ट्रैक करके, ग्राहक की पूरी यात्रा में क्रेडिट वितरित करने के लिए विभिन्न एट्रिब्यूशन मॉडल का उपयोग करके।

Key Concepts:

- **Customer Journey:**

  The path a customer takes from initial awareness to purchase, often involving multiple interactions with different marketing channels.
- **Touchpoints:**

  Specific interactions a customer has with a brand's marketing efforts, such as clicking on an ad, visiting a website, or opening an email.
- **Conversion:**

  A desired action a customer takes, such as making a purchase, signing up for a newsletter, or downloading an app.
- **Attribution Models:**
  Different methods used to assign credit to various touchpoints in the customer journey. Common models include Last-Click, First-Click, Linear, and Time Decay.

● ग्राहक यात्रा:

ग्राहक प्रारंभिक जागरूकता से लेकर खरीदारी तक का वह मार्ग अपनाता है, जिसमें अक्सर विभिन्न मार्केटिंग चैनलों के साथ कई इंटरैक्शन शामिल होते हैं।

● टचपॉइंट:

ग्राहक द्वारा ब्रांड के मार्केटिंग प्रयासों के साथ की जाने वाली विशिष्ट बातचीत, जैसे किसी विज्ञापन पर क्लिक करना, किसी वेबसाइट पर जाना या ईमेल खोलना।

● रूपांतरण:

ग्राहक द्वारा की जाने वाली कोई वांछित कार्रवाई, जैसे खरीदारी करना, न्यूज़लेटर के लिए साइन अप करना या ऐप डाउनलोड करना।

● एट्रिब्यूशन मॉडल:

ग्राहक यात्रा में विभिन्न टचपॉइंट्स को श्रेय देने के लिए उपयोग की जाने वाली विभिन्न विधियाँ। सामान्य मॉडलों में अंतिम-क्लिक, प्रथम-क्लिक, रैखिक और समय क्षय शामिल हैं।

How it Works

1. Track Customer Interactions:

Record all touchpoints a customer interacts with, such as clicking a social media ad, searching on Google, opening an email, or visiting a website directly.

2. Apply Attribution Models:

Use different models to assign value to these touchpoints based on various rules.

3. Evaluate Performance:

Analyze the data to understand the effectiveness of each marketing channel and campaign.

4. Optimize Spending:

Use these insights to adjust marketing spend, investing more in high-performing channels and reducing efforts on underperforming ones.

1. ग्राहक इंटरैक्शन ट्रैक करें:

ग्राहक जिन सभी टचपॉइंट्स से इंटरैक्ट करता है, उन्हें रिकॉर्ड करें, जैसे कि सोशल मीडिया विज्ञापन पर क्लिक करना, Google पर सर्च करना, ईमेल खोलना या सीधे किसी वेबसाइट पर जाना।

2. एट्रिब्यूशन मॉडल लागू करें:

विभिन्न नियमों के आधार पर इन टचपॉइंट्स को मान निर्दिष्ट करने के लिए विभिन्न मॉडलों का उपयोग करें।

3. प्रदर्शन का मूल्यांकन करें:

प्रत्येक मार्केटिंग चैनल और अभियान की प्रभावशीलता को समझने के लिए डेटा का विश्लेषण करें।

4. खर्च अनुकूलित करें:
मार्केटिंग खर्च को समायोजित करने, उच्च प्रदर्शन करने वाले चैनलों में अधिक निवेश करने और कम प्रदर्शन करने वाले चैनलों पर प्रयासों को कम करने के लिए इन जानकारियों का उपयोग करें।

Common Attribution Models

First-Touch Attribution

The first touch attribution model assigns 100% of conversion credit to the first marketing touchpoint in the customer journey. This single touch attribution approach excels at measuring top-of-funnel performance, making it ideal for identifying which marketing channels drive initial brand discovery and awareness.

फ़र्स्ट-टच एट्रिब्यूशन मॉडल, ग्राहक यात्रा के पहले मार्केटिंग टचपॉइंट को 100% रूपांतरण क्रेडिट प्रदान करता है। यह सिंगल-टच एट्रिब्यूशन दृष्टिकोण फ़नल के शीर्ष पर प्रदर्शन को मापने में उत्कृष्ट है, जिससे यह यह पहचानने के लिए आदर्श है कि कौन से मार्केटिंग चैनल प्रारंभिक ब्रांड खोज और जागरूकता को बढ़ावा देते हैं।

Last-Touch Attribution

Last click attribution gives all conversion credit to the final touchpoint before purchase. This is the default attribution model in Google Analytics and most ecommerce platforms, making it the most commonly used approach despite its limitations.

अंतिम क्लिक एट्रिब्यूशन, खरीदारी से पहले सभी रूपांतरणों का श्रेय अंतिम टचपॉइंट को देता है। यह Google Analytics और अधिकांश ई-कॉमर्स प्लेटफ़ॉर्म में डिफ़ॉल्ट एट्रिब्यूशन मॉडल है, जो अपनी सीमाओं के बावजूद इसे सबसे अधिक इस्तेमाल किया जाने वाला तरीका बनाता है।

Linear Attribution

Linear attribution distributes conversion credit equally across all touchpoints in the customer journey. This multi touch attribution model provides a balanced view of all marketing efforts without favoring any particular stage of the sales funnel.

लीनियर एट्रिब्यूशन, ग्राहक यात्रा के सभी टचपॉइंट्स पर रूपांतरण क्रेडिट को समान रूप से वितरित करता है। यह मल्टी-टच एट्रिब्यूशन मॉडल, बिक्री फ़नल के किसी विशेष चरण को प्राथमिकता दिए बिना, सभी मार्केटिंग प्रयासों का एक संतुलित दृष्टिकोण प्रदान करता है।

Time Decay Attribution

The time decay attribution model credits touchpoints more heavily as they get closer to the conversion event. This approach recognizes that recent interactions typically have stronger influence on immediate purchase decisions.

टाइम डेके एट्रिब्यूशन मॉडल, रूपांतरण घटना के करीब आने पर टचपॉइंट्स को ज़्यादा महत्व देता है। यह दृष्टिकोण यह मानता है कि हाल के इंटरैक्शन आमतौर पर तत्काल खरीदारी के फैसलों पर ज़्यादा प्रभाव डालते हैं।

Position-Based (U-Shaped) Attribution

Position based attribution typically distributes 40% credit each to the first and last touchpoints, with the remaining 20% spread across middle interactions. This model balances the importance of customer acquisition and conversion activities.

स्थिति-आधारित एट्रिब्यूशन आमतौर पर पहले और आखिरी टचपॉइंट्स को 40% क्रेडिट देता है, जबकि बाकी 20% मध्य इंटरैक्शन में बाँटा जाता है। यह मॉडल ग्राहक अधिग्रहण और रूपांतरण गतिविधियों के महत्व को संतुलित करता है।

W-Shaped Attribution

W-shaped attribution credits first touch (30%), lead creation (30%), opportunity creation (30%), and distributes the remaining 10% across other customer touchpoints. This model is designed for longer B2B ecommerce sales cycles with clearly defined milestone events.

डब्ल्यू-आकार का एट्रिब्यूशन पहले संपर्क (30%), लीड निर्माण (30%), अवसर निर्माण (30%) को श्रेय देता है, और शेष 10% को अन्य ग्राहक संपर्क बिंदुओं में वितरित करता है। यह मॉडल स्पष्ट रूप से परिभाषित माइलस्टोन इवेंट्स के साथ लंबे B2B ई-कॉमर्स बिक्री चक्रों के लिए डिज़ाइन किया गया है।

Data-Driven Attribution

Data driven attribution employs machine learning algorithms to analyze historical conversion data and automatically assign credit based on each touchpoint's actual influence on conversions. This represents the most sophisticated approach to marketing attribution modeling.

डेटा-संचालित एट्रिब्यूशन, ऐतिहासिक रूपांतरण डेटा का विश्लेषण करने और रूपांतरणों पर प्रत्येक टचपॉइंट के वास्तविक प्रभाव के आधार पर स्वचालित रूप से क्रेडिट प्रदान करने के लिए मशीन लर्निंग एल्गोरिदम का उपयोग करता है। यह मार्केटिंग एट्रिब्यूशन मॉडलिंग का सबसे परिष्कृत तरीका है।

Benefits of Attribution:

- **Improved ROI:**
  By understanding which channels are driving the most sales, businesses can optimize their spending and improve their return on investment.
- **Better Campaign Performance:**
  Attribution helps identify what's working and what's not, allowing for adjustments to improve overall campaign effectiveness.
- **Data-Driven Decisions:**

Attribution provides valuable data to make informed decisions about marketing strategies and budget allocation.

- **Customer Understanding:**
  It helps gain insights into customer behavior and how they interact with different marketing channels.
  In essence, attribution is crucial for e-commerce businesses to understand the impact of their marketing efforts and make data-driven decisions to improve performance and profitability.

एट्रिब्यूशन के लाभ:

● बेहतर ROI:

यह समझकर कि कौन से चैनल सबसे ज़्यादा बिक्री बढ़ा रहे हैं, व्यवसाय अपने खर्च को अनुकूलित कर सकते हैं और अपने निवेश पर लाभ में सुधार कर सकते हैं।

● बेहतर अभियान प्रदर्शन:

एट्रिब्यूशन यह पहचानने में मदद करता है कि क्या कारगर है और क्या नहीं, जिससे समग्र अभियान प्रभावशीलता में सुधार के लिए समायोजन संभव हो पाता है।

● डेटा-आधारित निर्णय:

एट्रिब्यूशन मार्केटिंग रणनीतियों और बजट आवंटन के बारे में सूचित निर्णय लेने के लिए मूल्यवान डेटा प्रदान करता है।

● ग्राहक समझ:

यह ग्राहक व्यवहार और विभिन्न मार्केटिंग चैनलों के साथ उनकी सहभागिता के बारे में जानकारी प्राप्त करने में मदद करता है।

संक्षेप में, ई-कॉमर्स व्यवसायों के लिए अपने मार्केटिंग प्रयासों के प्रभाव को समझने और प्रदर्शन एवं लाभप्रदता में सुधार के लिए डेटा-आधारित निर्णय लेने हेतु एट्रिब्यूशन महत्वपूर्ण है।

Acknowledgement

In e-commerce, an acknowledgement is a confirmation message sent to a buyer after they place an order, indicating that the seller has received and accepted the order. It serves as a receipt and also confirms the details of the order, such as the items, quantities, prices, and delivery information. This confirmation helps manage customer expectations and initiates the fulfillment process.

- **Receipt Confirmation:**

  An acknowledgement confirms that the seller has received the buyer's order.

- **Order Verification:**

  It allows the seller to verify the order details and identify any potential issues, such as out-of-stock items or incorrect information.

- **Communication of Intent:**

  The acknowledgement signifies the seller's intent to fulfill the order.

- **Fulfillment Process Initiation:**

  It triggers the next steps in the order fulfillment process, such as processing the payment and preparing the items for shipment.
- **Customer Satisfaction:**

  By providing timely and accurate acknowledgements, e-commerce businesses can improve customer satisfaction and build trust.
- **Example:**
  When a customer purchases a product on an e-commerce website, they typically receive an email or a message on the website confirming their order and providing details like order number, items, quantity, price, and delivery address.

ई-कॉमर्स में, पावती एक पुष्टिकरण संदेश होता है जो खरीदार द्वारा ऑर्डर देने के बाद भेजा जाता है, यह दर्शाता है कि विक्रेता ने ऑर्डर प्राप्त कर लिया है और उसे स्वीकार कर लिया है। यह एक रसीद के रूप में कार्य करता है और ऑर्डर के विवरण, जैसे कि आइटम, मात्रा, मूल्य और डिलीवरी की जानकारी, की पुष्टि भी करता है। यह पुष्टिकरण ग्राहक की अपेक्षाओं को प्रबंधित करने और पूर्ति प्रक्रिया शुरू करने में मदद करता है।

● रसीद की पुष्टि:
पावती यह पुष्टि करती है कि विक्रेता को खरीदार का ऑर्डर प्राप्त हो गया है।
● ऑर्डर सत्यापन:
यह विक्रेता को ऑर्डर विवरणों को सत्यापित करने और किसी भी संभावित समस्या, जैसे कि स्टॉक में न होने वाली वस्तुएँ या गलत जानकारी, की पहचान करने की अनुमति देता है।
● आशय का संचार:
पावती विक्रेता के ऑर्डर को पूरा करने के इरादे को दर्शाती है।
● पूर्ति प्रक्रिया आरंभ:
यह ऑर्डर पूर्ति प्रक्रिया के अगले चरणों को शुरू करता है, जैसे भुगतान संसाधित करना और शिपमेंट के लिए आइटम तैयार करना।
● ग्राहक संतुष्टि:
समय पर और सटीक पावती प्रदान करके, ई-कॉमर्स व्यवसाय ग्राहक संतुष्टि में सुधार कर सकते हैं और विश्वास का निर्माण कर सकते हैं।
● उदाहरण:
जब कोई ग्राहक किसी ई-कॉमर्स वेबसाइट पर कोई उत्पाद खरीदता है, तो उसे आमतौर पर वेबसाइट पर एक ईमेल या संदेश प्राप्त होता है जिसमें उसके ऑर्डर की पुष्टि होती है और ऑर्डर नंबर, आइटम, मात्रा, कीमत और डिलीवरी पता जैसी जानकारी दी जाती है।

Dispatch of electronic records

In e-commerce, the "dispatch of electronic records" refers to the point at which an electronic document is considered to be sent, as defined by legal frameworks like the Indian IT Act. It's a crucial concept for determining the timing and location of electronic transactions, especially for establishing legal validity and resolving potential disputes. Essentially, an electronic record is considered dispatched when it enters a computer system outside the sender's control.

Key Aspects of Dispatch in E-commerce:

- **Beyond Originator's Control:**

  The defining characteristic of dispatch is that the electronic record has moved from the sender's control and entered a system (e.g., a recipient's computer, an intermediary's server).

- **Time of Dispatch:**

  The time of dispatch is usually when the electronic record is sent, regardless of when it was created or composed. For example, even if an email is written earlier, it's dispatched when the "send" button is pressed.

- **Place of Dispatch:**

  The place of dispatch is generally considered to be the sender's place of business, according to some legal frameworks.

- **Importance in E-commerce:**
  Understanding the dispatch of electronic records is vital for:
- **Determining the start of a transaction:** When a contract is formed, when a payment is initiated, etc.
- **Establishing legal obligations:** Knowing when a message is "sent" helps determine if a party has met their obligations.
- **Resolving disputes:** If a disagreement arises about when an electronic record was sent, the rules for dispatch provide a clear framework for determining the time and location of the action.

Example:

Imagine a customer placing an order on an e-commerce website. The time they click "confirm order" is the point of dispatch for the electronic record of that order. This record is considered dispatched when it enters the website's system (a computer resource outside the customer's control)

ई-कॉमर्स में, "इलेक्ट्रॉनिक रिकॉर्ड का प्रेषण" उस बिंदु को संदर्भित करता है जिस पर किसी इलेक्ट्रॉनिक दस्तावेज़ को भेजा हुआ माना जाता है, जैसा कि भारतीय आईटी अधिनियम जैसे कानूनी ढाँचों द्वारा परिभाषित किया गया है। यह इलेक्ट्रॉनिक लेनदेन के समय और स्थान का निर्धारण करने के लिए, विशेष रूप से कानूनी वैधता स्थापित करने और संभावित विवादों को

सुलझाने के लिए, एक महत्वपूर्ण अवधारणा है। मूलतः, एक इलेक्ट्रॉनिक रिकॉर्ड तब भेजा हुआ माना जाता है जब वह प्रेषक के नियंत्रण से बाहर किसी कंप्यूटर सिस्टम में प्रवेश करता है।

ई-कॉमर्स में प्रेषण के प्रमुख पहलू:

- स्रोत के नियंत्रण से परे:

प्रेषण की विशिष्ट विशेषता यह है कि इलेक्ट्रॉनिक रिकॉर्ड प्रेषक के नियंत्रण से हटकर किसी सिस्टम (जैसे, प्राप्तकर्ता का कंप्यूटर, मध्यस्थ का सर्वर) में प्रवेश कर जाता है।

- प्रेषण का समय:

प्रेषण का समय आमतौर पर वह होता है जब इलेक्ट्रॉनिक रिकॉर्ड भेजा जाता है, चाहे वह कब बनाया या लिखा गया हो। उदाहरण के लिए, यदि कोई ईमेल पहले भी लिखा गया हो, तो "भेजें" बटन दबाने पर उसे भेज दिया जाता है।

- प्रेषण का स्थान:

कुछ कानूनी ढाँचों के अनुसार, प्रेषण का स्थान आमतौर पर प्रेषक का व्यावसायिक स्थान माना जाता है।

- ई-कॉमर्स में महत्व:

इलेक्ट्रॉनिक रिकॉर्ड के प्रेषण को समझना निम्नलिखित के लिए महत्वपूर्ण है:

- लेन-देन की शुरुआत का निर्धारण: अनुबंध कब बनता है, भुगतान कब शुरू होता है, आदि।
- कानूनी दायित्व स्थापित करना: यह जानना कि संदेश कब "भेजा" गया है, यह निर्धारित करने में मदद करता है कि क्या किसी पक्ष ने अपने दायित्वों को पूरा किया है।
- विवादों का समाधान: यदि इलेक्ट्रॉनिक रिकॉर्ड भेजे जाने के समय को लेकर असहमति उत्पन्न होती है, तो प्रेषण के नियम कार्रवाई के समय और स्थान को निर्धारित करने के लिए एक स्पष्ट रूपरेखा प्रदान करते हैं।

उदाहरण: कल्पना कीजिए कि कोई ग्राहक किसी ई-कॉमर्स वेबसाइट पर ऑर्डर देता है। जिस समय वे "ऑर्डर की पुष्टि करें" पर क्लिक करते हैं, उस ऑर्डर का इलेक्ट्रॉनिक रिकॉर्ड भेजने का समय वही होता है। यह रिकॉर्ड तब भेजा हुआ माना जाता है जब यह वेबसाइट के सिस्टम (ग्राहक के नियंत्रण से बाहर एक कंप्यूटर संसाधन) में पहुँच जाता है।

Regulation of certifying authorities:-

The contemporary landscape is defined by the relentless march of science and technology, shaping a world that is increasingly digital, efficient, and interconnected. In this era, our lives have been streamlined, made faster and smarter through the utilization of digital documents. Institutions and organizations have embraced online modes of communication, facilitated by certifying authorities. These trusted entities issue digital certificates, ensuring the legitimacy of electronic documents and the identities they represent. Operating under a web of rules and regulations of certifying authority are the linchpin in maintaining the smooth functioning of the digital realm.

Certifying Authorities (CAs) in India are regulated under the Information Technology Act, 2000, and the Controller of Certifying Authorities (CCA) is the key regulatory body. The CCA, appointed by the Central Government, oversees the licensing, operation, and compliance of CAs, ensuring they adhere to the prescribed standards and procedures. This regulation aims to build trust and security in digital transactions by verifying the identities of individuals and organizations using digital signatures.

समकालीन परिदृश्य विज्ञान और प्रौद्योगिकी की निरंतर प्रगति द्वारा परिभाषित है, जो एक ऐसी दुनिया को आकार दे रहा है जो तेज़ी से डिजिटल, कुशल और परस्पर जुड़ी हुई है। इस युग में, डिजिटल दस्तावेज़ों के उपयोग से हमारा जीवन सुव्यवस्थित, तेज़ और स्मार्ट हो गया है। संस्थानों और संगठनों ने प्रमाणन प्राधिकरणों द्वारा सुगम बनाए गए ऑनलाइन संचार माध्यमों को अपनाया है। ये विश्वसनीय संस्थाएँ डिजिटल प्रमाणपत्र जारी करती हैं, जिससे इलेक्ट्रॉनिक दस्तावेज़ों और उनकी पहचान की वैधता सुनिश्चित होती है। प्रमाणन प्राधिकरण के नियमों और विनियमों के जाल के तहत काम करना डिजिटल क्षेत्र के सुचारू संचालन को बनाए रखने में महत्वपूर्ण भूमिका निभाता है।

भारत में प्रमाणन प्राधिकरण (CA) सूचना प्रौद्योगिकी अधिनियम, 2000 के तहत विनियमित होते हैं, और प्रमाणन प्राधिकरण नियंत्रक (CCA) प्रमुख नियामक निकाय है। केंद्र सरकार द्वारा नियुक्त CCA, CA के लाइसेंसिंग, संचालन और अनुपालन की देखरेख करता है, यह सुनिश्चित करता है कि वे निर्धारित मानकों और प्रक्रियाओं का पालन करें। इस विनियमन का उद्देश्य डिजिटल हस्ताक्षरों का उपयोग करके व्यक्तियों और संगठनों की पहचान सत्यापित करके डिजिटल लेनदेन में विश्वास और सुरक्षा का निर्माण करना है।

- **Licensing and Oversight:**

  The CCA grants and revokes licenses for CAs, ensuring they meet the necessary infrastructure and security requirements.

  लाइसेंसिंग और निरीक्षण:

  सीसीए, सीए को लाइसेंस प्रदान और निरस्त करता है, यह सुनिश्चित करते हुए कि वे आवश्यक बुनियादी ढाँचे और सुरक्षा आवश्यकताओं को पूरा करते हैं।

- **Standards and Procedures:**

  CAs must adhere to specific standards and procedures, including using secure hardware, software, and maintaining the secrecy and privacy of digital signatures.

  मानक और प्रक्रियाएँ:

  सीए को विशिष्ट मानकों और प्रक्रियाओं का पालन करना होगा, जिसमें सुरक्षित हार्डवेयर, सॉफ़्टवेयर का उपयोग और डिजिटल हस्ताक्षरों की गोपनीयता और निजता बनाए रखना शामिल है।

- **Supervision and Audits:**

  The CCA supervises CA operations, conducts audits, and resolves disputes between CAs and subscribers.

  पर्यवेक्षण और लेखा परीक्षा:

  सीसीए, सीए के कार्यों का पर्यवेक्षण करता है, लेखा परीक्षा करता है, और सीए और ग्राहकों के बीच विवादों का समाधान करता है।

- **Suspension and Revocation:**

  The CCA can suspend or revoke a CA's license for failing to comply with regulations or for other specified reasons, after providing an opportunity to be heard.

  निलंबन और निरसन:

  सीसीए, सुनवाई का अवसर प्रदान करने के बाद, विनियमों का पालन न करने या अन्य निर्दिष्ट कारणों से, सीए का लाइसेंस निलंबित या निरस्त कर सकता है।

- **Key Pair Management:**

  CAs are required to manage their key pairs (private and public) securely, including changing them periodically and handling compromises appropriately.

  कुंजी जोड़ी प्रबंधन:

  CA को अपने कुंजी युग्मों (निजी और सार्वजनिक) को सुरक्षित रूप से प्रबंधित करना आवश्यक है, जिसमें उन्हें समय-समय पर बदलना और उचित रूप से समझौता करना शामिल है।

- **Certificate Revocation Lists (CRLs):**

  CAs maintain CRLs to list invalid or revoked certificates, ensuring users can verify the validity of digital signatures.

  प्रमाणपत्र निरस्तीकरण सूची (सीआरएल):

  CA अमान्य या निरस्त प्रमाणपत्रों को सूचीबद्ध करने के लिए CRLs बनाए रखते हैं, जिससे यह सुनिश्चित होता है कि उपयोगकर्ता डिजिटल हस्ताक्षरों की वैधता को सत्यापित कर सकें।

- **Subscriber Responsibilities:**
  Subscribers also have responsibilities, such as maintaining the secrecy of their private keys and ensuring their information is accurate when applying for certificates.

  सब्सक्राइबर की ज़िम्मेदारियाँ:

  सब्सक्राइबर की भी ज़िम्मेदारियाँ होती हैं, जैसे कि अपनी निजी कुंजियों की गोपनीयता बनाए रखना और प्रमाणपत्र के लिए आवेदन करते समय यह सुनिश्चित करना कि उनकी जानकारी सटीक है।

Role of the Controller of Certifying Authorities (CCA):

The CCA plays a central role in regulating the digital signature infrastructure in India. Its functions include:

- **Granting and revoking licenses for CAs:** Ensuring only qualified entities operate as CAs.
- **Setting standards and guidelines for CAs:** Establishing the rules and procedures CAs must follow.
- **Supervising and auditing CA operations:** Monitoring compliance and identifying potential issues.
- **Resolving disputes between CAs and subscribers:** Acting as an intermediary to resolve disagreements.
- **Maintaining a database of public keys:** Providing a central repository for public keys issued by CAs.
  In essence, the regulation of CAs in India focuses on ensuring trust, security, and reliability in digital transactions by:
- Establishing a robust framework for licensing and oversight of CAs.
- Setting clear standards and procedures for CA operations.
- Providing mechanisms for addressing non-compliance and resolving disputes.
- Empowering subscribers with the knowledge and tools to utilize digital signatures securely.

प्रमाणन प्राधिकरण नियंत्रक (CCA) की भूमिका:

भारत में डिजिटल हस्ताक्षर अवसंरचना के विनियमन में CCA एक केंद्रीय भूमिका निभाता है। इसके कार्यों में शामिल हैं:

● CA के लिए लाइसेंस प्रदान करना और रद्द करना: यह सुनिश्चित करना कि केवल योग्य संस्थाएँ ही CA के रूप में कार्य करें।

● CA के लिए मानक और दिशानिर्देश निर्धारित करना: CA द्वारा पालन किए जाने वाले नियम और प्रक्रियाएँ निर्धारित करना।

● CA संचालन का पर्यवेक्षण और लेखा-परीक्षण: अनुपालन की निगरानी और संभावित समस्याओं की पहचान करना।

● CA और ग्राहकों के बीच विवादों का समाधान: मतभेदों को सुलझाने के लिए मध्यस्थ के रूप में कार्य करना।

● सार्वजनिक कुंजियों का डेटाबेस बनाए रखना: CA द्वारा जारी सार्वजनिक कुंजियों के लिए एक केंद्रीय भंडार प्रदान करना।

संक्षेप में, भारत में CA का विनियमन डिजिटल लेनदेन में विश्वास, सुरक्षा और विश्वसनीयता सुनिश्चित करने पर केंद्रित है:

● CA के लाइसेंस और निगरानी के लिए एक मजबूत ढाँचा स्थापित करना।
● CA संचालन के लिए स्पष्ट मानक और प्रक्रियाएँ निर्धारित करना।
● गैर-अनुपालन को संबोधित करने और विवादों को सुलझाने के लिए तंत्र प्रदान करना।
● डिजिटल हस्ताक्षरों का सुरक्षित उपयोग करने के लिए ज्ञान और उपकरणों के साथ ग्राहकों को सशक्त बनाना।

DIGITAL SIGNATURE CERTIFICATE:-

A Digital Signature Certificate(DSC) is an electronic and legal alternative of traditional wet signature. It can be presented electronically to obtain services or information on the internet or else to sign documents digitally. Also, users can utilize a digital signature certificate to send encrypted emails. A digital signature certificate authenticates the signer's details necessary to generate a digital signature. Most importantly, a digital signature certificate is highly secure file that stores signer's personal information.

An individual or an organization can be eligible to digitally sign documents only after registering with a Certifying Authority (CA). A certifying authority is an organization authorized to issue digital signature certificates, licensed by the Controller of Certifying Authority (CCA). eMudhra is a licensed certifying authority wherein, individuals or organizations can purchase class 3 digital signature certificates for one, two, or three years.

A class 3 digital signature certificate is necessary for GST, income tax, e-procurement, EPFO filing, tender submissions, and much more. The entire registration process for the purchase of a digital signature certificate is conducted online on the eMudhra website. eMudhra deploys multi-factor authentication to verify the user identity in less than 5 minutes. After verification, the digital signature certificate is made available for download within 30 minutes.

डिजिटल हस्ताक्षर प्रमाणपत्र (DSC) पारंपरिक वेट सिग्नेचर का एक इलेक्ट्रॉनिक और कानूनी विकल्प है। इसे इंटरनेट पर सेवाएँ या जानकारी प्राप्त करने या दस्तावेज़ों पर डिजिटल रूप से हस्ताक्षर करने के लिए इलेक्ट्रॉनिक रूप से प्रस्तुत किया जा सकता है। इसके अलावा, उपयोगकर्ता एन्क्रिप्टेड ईमेल भेजने के लिए डिजिटल हस्ताक्षर प्रमाणपत्र का उपयोग कर सकते हैं। एक डिजिटल हस्ताक्षर प्रमाणपत्र, डिजिटल हस्ताक्षर बनाने के लिए आवश्यक हस्ताक्षरकर्ता के विवरणों को प्रमाणित करता है। सबसे महत्वपूर्ण बात यह है कि एक डिजिटल हस्ताक्षर प्रमाणपत्र एक अत्यधिक सुरक्षित फ़ाइल होती है जो हस्ताक्षरकर्ता की व्यक्तिगत जानकारी संग्रहीत करती है।
कोई व्यक्ति या संगठन केवल प्रमाणन प्राधिकरण (CA) के साथ पंजीकरण करने के बाद ही दस्तावेज़ों पर डिजिटल हस्ताक्षर करने के लिए पात्र हो सकता है। प्रमाणन प्राधिकरण एक ऐसा संगठन होता है जो डिजिटल हस्ताक्षर प्रमाणपत्र जारी करने के लिए अधिकृत होता है, और प्रमाणन प्राधिकरण नियंत्रक (CCA) द्वारा लाइसेंस प्राप्त होता है। eMudhra एक लाइसेंस प्राप्त

प्रमाणन प्राधिकरण है, जहाँ व्यक्ति या संगठन एक, दो या तीन वर्षों के लिए क्लास 3 डिजिटल हस्ताक्षर प्रमाणपत्र खरीद सकते हैं।
GST, आयकर, ई-प्रोक्योरमेंट, EPFO फाइलिंग, निविदा प्रस्तुतियाँ, आदि के लिए क्लास 3 डिजिटल हस्ताक्षर प्रमाणपत्र आवश्यक है। डिजिटल हस्ताक्षर प्रमाणपत्र की खरीद के लिए पूरी पंजीकरण प्रक्रिया eMudhra वेबसाइट पर ऑनलाइन आयोजित की जाती है। eMudhra उपयोगकर्ता की पहचान को 5 मिनट से भी कम समय में सत्यापित करने के लिए बहु-कारक प्रमाणीकरण का उपयोग करता है। सत्यापन के बाद, डिजिटल हस्ताक्षर प्रमाणपत्र 30 मिनट के भीतर डाउनलोड के लिए उपलब्ध करा दिया जाता है।

Digital Signatures and Certificates

Digital signatures and certificates are two key technologies that play an important role in ensuring the security and authenticity of online activities. They are essential for activities such as online banking, secure email communication, software distribution, and electronic document signing. By providing mechanisms for authentication, integrity, and non-repudiation, these technologies help protect against fraud, data breaches, and unauthorized access.

Experience the ease of obtaining legally binding signatures online, all while maintaining the highest standards of security and compliance with the leading e-signature platform, SignNow. It is a secure and efficient electronic signature solution designed to streamline your document signing process while ensuring top-tier security features.

डिजिटल हस्ताक्षर और प्रमाणपत्र दो प्रमुख तकनीकें हैं जो ऑनलाइन गतिविधियों की सुरक्षा और प्रामाणिकता सुनिश्चित करने में महत्वपूर्ण भूमिका निभाती हैं। ये ऑनलाइन बैंकिंग, सुरक्षित ईमेल संचार, सॉफ़्टवेयर वितरण और इलेक्ट्रॉनिक दस्तावेज़ हस्ताक्षर जैसी गतिविधियों के लिए आवश्यक हैं। प्रमाणीकरण, अखंडता और अस्वीकृति-रहित तंत्र प्रदान करके, ये तकनीकें धोखाधड़ी, डेटा उल्लंघनों और अनधिकृत पहुँच से सुरक्षा प्रदान करने में मदद करती हैं।

अग्रणी ई-हस्ताक्षर प्लेटफ़ॉर्म, SignNow के साथ सुरक्षा और अनुपालन के उच्चतम मानकों को बनाए रखते हुए, ऑनलाइन कानूनी रूप से बाध्यकारी हस्ताक्षर प्राप्त करने की आसानी का अनुभव करें। यह एक सुरक्षित और कुशल इलेक्ट्रॉनिक हस्ताक्षर समाधान है जिसे आपकी दस्तावेज़ हस्ताक्षर प्रक्रिया को सुव्यवस्थित करने और शीर्ष-स्तरीय सुरक्षा सुविधाएँ सुनिश्चित करने के लिए डिज़ाइन किया गया है।

Digital Signature

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document. These are some of the key features of it.

डिजिटल हस्ताक्षर एक गणितीय तकनीक है जिसका उपयोग किसी संदेश, सॉफ़्टवेयर या डिजिटल दस्तावेज़ की प्रामाणिकता और अखंडता की पुष्टि के लिए किया जाता है। ये इसकी कुछ प्रमुख विशेषताएँ हैं।

- **Key Generation Algorithms**: Digital signatures are electronic signatures, which assure that the message was sent by a particular sender. While performing digital transactions authenticity and integrity should be assured, otherwise, the data can be altered or someone can also act as if he were the sender and expect a reply.
- **Signing Algorithms**: To create a digital signature, signing algorithms like email programs create a one-way hash of the electronic data which is to be signed. The signing algorithm then encrypts the hash value using the private key (signature key). This encrypted hash along with other information like the hashing algorithm is the digital signature. This digital signature is appended with the data and sent to the verifier. The reason for encrypting the hash instead of the entire message or document is that a hash function converts any arbitrary input into a much shorter fixed-length value. This saves time as now instead of signing a long message a shorter hash value has to be signed and hashing is much faster than signing.
- **Signature Verification Algorithms**: The Verifier receives a Digital Signature along with the data. It then uses a Verification algorithm to process the digital signature and the public key (verification key) and generates some value. It also applies the same hash function on the received data and generates a hash value. If they both are equal, then the digital signature is valid else it is invalid.

● कुंजी निर्माण एल्गोरिदम: डिजिटल हस्ताक्षर इलेक्ट्रॉनिक हस्ताक्षर होते हैं, जो यह सुनिश्चित करते हैं कि संदेश किसी विशिष्ट प्रेषक द्वारा भेजा गया है। डिजिटल लेनदेन करते समय प्रामाणिकता और अखंडता सुनिश्चित की जानी चाहिए, अन्यथा, डेटा में बदलाव किया जा सकता है या कोई व्यक्ति प्रेषक की तरह व्यवहार कर सकता है और उत्तर की अपेक्षा कर सकता है।

● हस्ताक्षर एल्गोरिदम: डिजिटल हस्ताक्षर बनाने के लिए, ईमेल प्रोग्राम जैसे हस्ताक्षर एल्गोरिदम, हस्ताक्षरित किए जाने वाले इलेक्ट्रॉनिक डेटा का एक-तरफ़ा हैश बनाते हैं। हस्ताक्षर एल्गोरिदम फिर निजी कुंजी (हस्ताक्षर कुंजी) का उपयोग करके हैश मान को एन्क्रिप्ट करता है।

यह एन्क्रिप्टेड हैश, हैशिंग एल्गोरिदम जैसी अन्य जानकारी के साथ, डिजिटल हस्ताक्षर कहलाता है। इस डिजिटल हस्ताक्षर को डेटा के साथ जोड़कर सत्यापनकर्ता को भेजा जाता है। पूरे संदेश या दस्तावेज़ के बजाय हैश को एन्क्रिप्ट करने का कारण यह है कि हैश फ़ंक्शन किसी भी मनमाने इनपुट को बहुत छोटे, निश्चित-लंबाई वाले मान में परिवर्तित कर देता है। इससे समय की बचत होती है क्योंकि अब लंबे संदेश पर हस्ताक्षर करने के बजाय एक छोटे हैश मान पर हस्ताक्षर करना पड़ता है और हैशिंग, हस्ताक्षर करने की तुलना में बहुत तेज़ है।

● हस्ताक्षर सत्यापन एल्गोरिदम: सत्यापनकर्ता को डेटा के साथ एक डिजिटल हस्ताक्षर भी प्राप्त होता है। फिर वह डिजिटल हस्ताक्षर और सार्वजनिक कुंजी (सत्यापन कुंजी) को संसाधित करने के लिए एक सत्यापन एल्गोरिदम का उपयोग करता है और कुछ मान उत्पन्न करता है। वह प्राप्त डेटा पर भी वही हैश फ़ंक्शन लागू करता है और एक हैश मान उत्पन्न करता है। यदि दोनों समान हैं, तो डिजिटल हस्ताक्षर मान्य है अन्यथा यह अमान्य है।

How Digital Signature Works

The steps followed in creating a digital signature are:

1. Message digest is computed by applying the hash function on the message and then message digest is encrypted using the private key of the sender to form the digital signature. (digital signature = encryption (private key of sender, message digest) and message digest = message digest algorithm (message)).

2. A digital signature is then transmitted with the message. (message + digital signature is transmitted).

3. The receiver decrypts the digital signature using the public key of the sender. (This assures authenticity, as only the sender has his private key so only the sender can encrypt using his private key which can thus be decrypted by the sender’s public key).

4. The receiver now has the message digest.

5. The receiver can compute the message digest from the message (actual message is sent with the digital signature).
6. The message digest computed by receiver and the message digest (got by decryption on digital signature) need to be same for ensuring integrity.

Message digest is computed using one-way hash function, i.e. a hash function in which computation of hash value of a message is easy but computation of the message from hash value of the message is very difficult.

डिजिटल हस्ताक्षर बनाने के चरण इस प्रकार हैं:

1. संदेश पर हैश फ़ंक्शन लागू करके संदेश डाइजेस्ट की गणना की जाती है और फिर डिजिटल हस्ताक्षर बनाने के लिए प्रेषक की निजी कुंजी का उपयोग करके संदेश डाइजेस्ट को एन्क्रिप्ट किया जाता है। (डिजिटल हस्ताक्षर = एन्क्रिप्शन (प्रेषक की निजी कुंजी, संदेश डाइजेस्ट) और संदेश डाइजेस्ट = संदेश डाइजेस्ट एल्गोरिथम (संदेश))।

2. फिर संदेश के साथ एक डिजिटल हस्ताक्षर प्रेषित किया जाता है। (संदेश + डिजिटल हस्ताक्षर प्रेषित किया जाता है)।

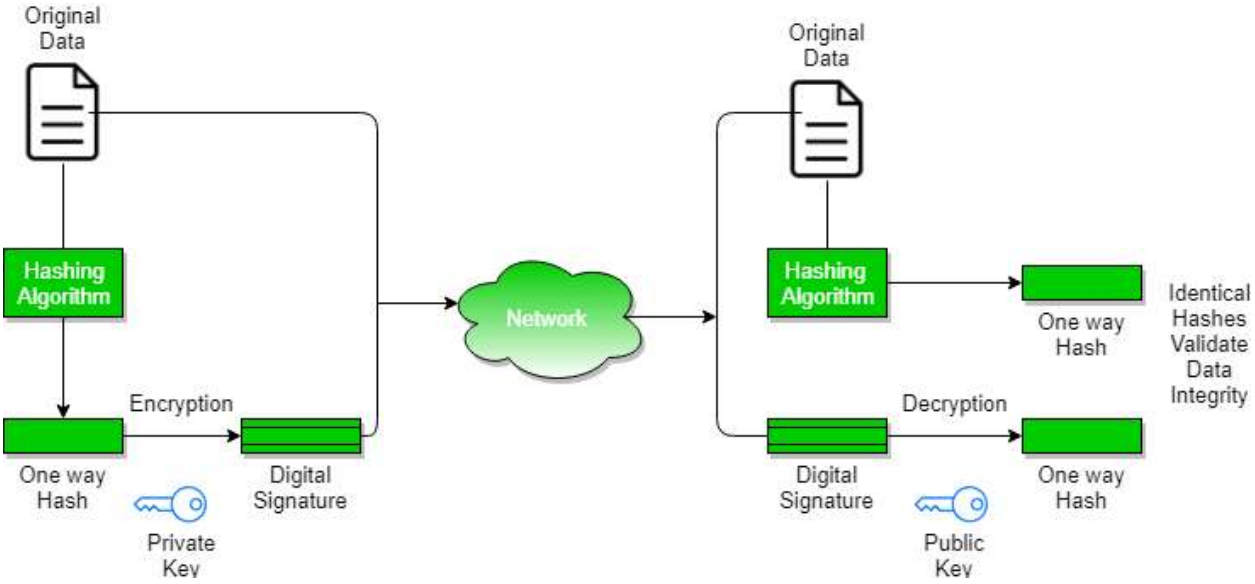
3. प्राप्तकर्ता प्रेषक की सार्वजनिक कुंजी का उपयोग करके डिजिटल हस्ताक्षर को डिक्रिप्ट करता है। (यह प्रामाणिकता सुनिश्चित करता है, क्योंकि केवल प्रेषक के पास ही उसकी निजी कुंजी होती है, इसलिए केवल प्रेषक ही अपनी निजी कुंजी का उपयोग करके एन्क्रिप्ट कर सकता है, जिसे इस प्रकार प्रेषक की सार्वजनिक कुंजी द्वारा डिक्रिप्ट किया जा सकता है)।

4. अब प्राप्तकर्ता के पास संदेश डाइजेस्ट होता है।

5. प्राप्तकर्ता संदेश से संदेश डाइजेस्ट की गणना कर सकता है (वास्तविक संदेश डिजिटल हस्ताक्षर के साथ भेजा जाता है)।

6. अखंडता सुनिश्चित करने के लिए प्राप्तकर्ता द्वारा गणना किया गया संदेश डाइजेस्ट और डिजिटल हस्ताक्षर पर डिक्रिप्शन द्वारा प्राप्त संदेश डाइजेस्ट समान होना चाहिए।

संदेश डाइजेस्ट की गणना एक-तरफ़ा हैश फ़ंक्शन का उपयोग करके की जाती है, अर्थात एक ऐसा हैश फ़ंक्शन जिसमें संदेश के हैश मान की गणना आसान होती है, लेकिन संदेश के हैश मान से संदेश की गणना करना बहुत कठिन होता है।



Benefits of Digital Signatures

- **Legal documents and contracts:** Digital signatures are legally binding. This makes them ideal for any legal document that requires a signature authenticated by one or more parties and guarantees that the record has not been altered.
- **Sales contracts:** Digital signing of contracts and sales contracts authenticates the identity of the seller and the buyer, and both parties can be sure that the signatures are legally binding and that the terms of the agreement have not been changed.
- **Financial Documents:** Finance departments digitally sign invoices so customers can trust that the payment request is from the right seller, not from a attacker trying to trick the buyer into sending payments to a fraudulent account.
- **Health Data:** In the healthcare industry, privacy is paramount for both patient records and research data. Digital signatures ensure that this confidential information was not modified when it was transmitted between the consenting parties.

डिजिटल हस्ताक्षर के लाभ

● कानूनी दस्तावेज़ और अनुबंध: डिजिटल हस्ताक्षर कानूनी रूप से **बाध्यकारी** होते हैं। यह उन्हें **ऐसे किसी भी कानूनी दस्तावेज़** के लिए आदर्श बनाता है जिसके लिए एक या अधिक पक्षों द्वारा **प्रमाणित हस्ताक्षर की आवश्यकता** होती है और यह गारंटी देता है कि रिकॉर्ड में कोई बदलाव नहीं किया गया है।

● बिक्री अनुबंध: अनुबंधों और बिक्री अनुबंधों पर डिजिटल हस्ताक्षर विक्रेता और खरीदार की पहचान प्रमाणित करते हैं, और दोनों पक्ष निश्चिंत हो सकते हैं कि हस्ताक्षर कानूनी रूप से बाध्यकारी हैं और समझौते की शर्तों में कोई बदलाव नहीं किया गया है।

● वित्तीय दस्तावेज़: वित्त विभाग चालानों पर डिजिटल हस्ताक्षर करते हैं ताकि ग्राहक यह विश्वास कर सकें कि भुगतान अनुरोध सही विक्रेता से है, न कि किसी हमलावर से जो खरीदार को धोखा देकर किसी धोखाधड़ी वाले खाते में भुगतान भेजने की कोशिश कर रहा है।

● स्वास्थ्य डेटा: स्वास्थ्य सेवा उद्योग में, रोगी रिकॉर्ड और अनुसंधान डेटा दोनों के लिए गोपनीयता सर्वोपरि है। डिजिटल हस्ताक्षर यह सुनिश्चित करते हैं कि सहमति देने वाले पक्षों के बीच प्रेषित होने पर इस गोपनीय जानकारी में कोई बदलाव नहीं किया गया हो।

Drawbacks of Digital Signature

- **Dependency on technology:** Because digital signatures rely on technology, they are susceptible to crimes, including hacking. As a result, businesses that use digital signatures must make sure their systems are safe and have the most recent security patches and upgrades installed.
- **Complexity:** Setting up and using digital signatures can be challenging, especially for those who are unfamiliar with the technology. This may result in blunders and errors that reduce the system's efficacy. The process of issuing digital signatures to senior citizens can occasionally be challenging.
- **Limited acceptance:** Digital signatures take time to replace manual ones since technology is not widely available in India, a developing nation.

डिजिटल हस्ताक्षर के नुकसान

● तकनीक पर निर्भरता: चूँकि डिजिटल हस्ताक्षर तकनीक पर निर्भर करते हैं, इसलिए वे हैकिंग सहित अपराधों के प्रति संवेदनशील होते हैं। परिणामस्वरूप, डिजिटल हस्ताक्षरों का उपयोग करने वाले व्यवसायों को यह सुनिश्चित करना होगा कि उनके सिस्टम सुरक्षित हों और उनमें नवीनतम सुरक्षा पैच और अपग्रेड इंस्टॉल हों।

● जटिलता: डिजिटल हस्ताक्षरों को सेट अप करना और उनका उपयोग करना चुनौतीपूर्ण हो सकता है, खासकर उन लोगों के लिए जो तकनीक से परिचित नहीं हैं। इसके परिणामस्वरूप ऐसी

गलतियाँ और त्रुटियाँ हो सकती हैं जो सिस्टम की प्रभावशीलता को कम कर देती हैं। वरिष्ठ नागरिकों को डिजिटल हस्ताक्षर जारी करने की प्रक्रिया कभी-कभी चुनौतीपूर्ण हो सकती है।

● सीमित स्वीकृति: डिजिटल हस्ताक्षरों को मैन्युअल हस्ताक्षरों की जगह लेने में समय लगता है क्योंकि विकासशील देश भारत में तकनीक व्यापक रूप से उपलब्ध नहीं है।

Digital Certificate

Digital certificate is issued by a trusted third party which proves sender's identity to the receiver and receiver's identity to the sender. A digital certificate is a certificate issued by a Certificate Authority (CA) to verify the identity of the certificate holder. Digital certificate is used to attach public key with a particular individual or an entity.

डिजिटल प्रमाणपत्र एक विश्वसनीय तृतीय पक्ष द्वारा जारी किया जाता है जो प्राप्तकर्ता को प्रेषक की पहचान और प्रेषक को प्राप्तकर्ता की पहचान प्रमाणित करता है। डिजिटल प्रमाणपत्र, प्रमाणपत्र धारक की पहचान सत्यापित करने के लिए प्रमाणपत्र प्राधिकरण (CA) द्वारा जारी किया गया एक प्रमाणपत्र होता है। डिजिटल प्रमाणपत्र का उपयोग किसी विशिष्ट व्यक्ति या संस्था के साथ सार्वजनिक कुंजी संलग्न करने के लिए किया जाता है।

Digital Certificate Contains

- Name of certificate holder.
- Serial number which is used to uniquely identify a certificate, the individual or the entity identified by the certificate
- Expiration dates.
- Copy of certificate holder's public key. (used for decrypting messages and digital signatures)
- Digital Signature of the certificate issuing authority.

Digital certificate is also sent with the digital signature and the message.

● प्रमाणपत्र धारक का नाम।

● क्रमांक जिसका उपयोग प्रमाणपत्र, प्रमाणपत्र द्वारा पहचाने गए व्यक्ति या संस्था की विशिष्ट पहचान के लिए किया जाता है।

● समाप्ति तिथियाँ।

● प्रमाणपत्र धारक की सार्वजनिक कुंजी की प्रति। (संदेशों और डिजिटल हस्ताक्षरों को डिक्रिप्ट करने के लिए उपयोग किया जाता है)

● प्रमाणपत्र जारी करने वाले प्राधिकारी का डिजिटल हस्ताक्षर।

डिजिटल प्रमाणपत्र भी डिजिटल हस्ताक्षर और संदेश के साथ भेजा जाता है।

Advantages of Digital Certificate

- **Network Security:** A complete layered strategy is required by modern cybersecurity methods, wherein many solutions cooperate to offer the highest level of protection against attackers. An essential component of this puzzle is digital certificates, which offer strong defense against manipulation and man-in-the-middle attacks.
- **Verification:** Digital certificates facilitate cybersecurity by restricting access to sensitive data, which makes authentication a crucial component of cybersecurity. Thus, there is a decreased chance that attackers will cause disturbance. At many different endpoints, certificate-based authentication provides a dependable method of identity verification. Compared to other popular authentication methods like biometrics or one-time passwords, certificates are more flexible.
- **Buyer Success:** Consumers demand complete assurance that the websites they visit are reliable. Because digital certificates are supported by certificate authority that users' browsers trust, they offer a readily identifiable indicator of reliability.

डिजिटल प्रमाणपत्र के लाभ

● नेटवर्क सुरक्षा: आधुनिक साइबर सुरक्षा विधियों के लिए एक संपूर्ण स्तरित रणनीति की आवश्यकता होती है, जिसमें कई समाधान मिलकर हमलावरों के विरुद्ध उच्चतम स्तर की सुरक्षा प्रदान करते हैं। इस पहेली का एक अनिवार्य घटक डिजिटल प्रमाणपत्र हैं, जो हेरफेर और मैन-इन-द-मिडिल हमलों के विरुद्ध मज़बूत सुरक्षा प्रदान करते हैं।

● सत्यापन: डिजिटल प्रमाणपत्र संवेदनशील डेटा तक पहुँच को प्रतिबंधित करके साइबर सुरक्षा को सुगम बनाते हैं, जिससे प्रमाणीकरण साइबर सुरक्षा का एक महत्वपूर्ण घटक बन जाता है। इस प्रकार, हमलावरों द्वारा व्यवधान उत्पन्न करने की संभावना कम हो जाती है। कई अलग-अलग अंतिम बिंदुओं पर, प्रमाणपत्र-आधारित प्रमाणीकरण पहचान सत्यापन का एक विश्वसनीय तरीका प्रदान करता है। बायोमेट्रिक्स या वन-टाइम पासवर्ड जैसी अन्य लोकप्रिय प्रमाणीकरण विधियों की तुलना में, प्रमाणपत्र अधिक लचीले होते हैं।

● खरीदार की सफलता: उपभोक्ता पूर्ण आश्वासन चाहते हैं कि वे जिन वेबसाइटों पर जाते हैं वे विश्वसनीय हैं। चूँकि डिजिटल प्रमाणपत्र प्रमाणपत्र प्राधिकरण द्वारा समर्थित होते हैं जिन पर उपयोगकर्ता के ब्राउज़र भरोसा करते हैं, वे विश्वसनीयता का एक आसानी से पहचाना जाने वाला संकेतक प्रदान करते हैं।

Disadvantages of Digital Certificate

- **Phishing Attacks:** To make their websites look authentic, attackers can fabricate bogus websites and obtain certificates. Users may be fooled into providing sensitive information, such as their login credentials, which the attacker may then take advantage of.
- **Weak Encryption:** Older digital certificate systems may employ less secure encryption methods that are open to intrusions.
- **Misconfiguration:** In order for digital certificates to work, they need to be set up correctly. Websites and online interactions can be attacked due to incorrectly configured certificates.

डिजिटल प्रमाणपत्र के नुकसान

● फ़िशिंग हमले: अपनी वेबसाइटों को प्रामाणिक दिखाने के लिए, हमलावर फर्जी वेबसाइटें बनाकर प्रमाणपत्र प्राप्त कर सकते हैं। उपयोगकर्ताओं को धोखा देकर उनसे संवेदनशील जानकारी, जैसे कि उनके लॉगिन क्रेडेंशियल, प्राप्त की जा सकती है, जिसका हमलावर फिर फायदा उठा सकता है।
● कमज़ोर एन्क्रिप्शन: पुरानी डिजिटल प्रमाणपत्र प्रणालियाँ कम सुरक्षित एन्क्रिप्शन विधियों का उपयोग कर सकती हैं जो घुसपैठ के लिए खुली होती हैं।
● गलत कॉन्फ़िगरेशन: डिजिटल प्रमाणपत्रों के काम करने के लिए, उन्हें सही तरीके से सेट अप किया जाना चाहिए। गलत तरीके से कॉन्फ़िगर किए गए प्रमाणपत्रों के कारण वेबसाइटों और ऑनलाइन इंटरैक्शन पर हमला हो सकता है।

Digital Certificate vs Digital Signature

Digital signature is used to verify authenticity, integrity, non-repudiation, i.e. it is assuring that the message is sent by the known user and not modified, while digital certificate is used to verify the identity of the user, maybe sender or receiver. Thus digital signature and certificate are different kind of things but both are used for security. Most websites use digital certificate to enhance trust of their users.

डिजिटल प्रमाणपत्र बनाम डिजिटल हस्ताक्षर

डिजिटल हस्ताक्षर का उपयोग प्रामाणिकता, अखंडता और अस्वीकृत न होने की पुष्टि के लिए किया जाता है, अर्थात यह सुनिश्चित करता है कि संदेश ज्ञात उपयोगकर्ता द्वारा भेजा गया है और उसमें कोई बदलाव नहीं किया गया है, जबकि डिजिटल प्रमाणपत्र का उपयोग उपयोगकर्ता, चाहे वह प्रेषक हो या प्राप्तकर्ता, की पहचान सत्यापित करने के लिए किया जाता है। इस प्रकार, डिजिटल हस्ताक्षर और प्रमाणपत्र अलग-अलग चीजें हैं, लेकिन दोनों का उपयोग सुरक्षा के लिए किया जाता है। अधिकांश वेबसाइटें अपने उपयोगकर्ताओं का विश्वास बढ़ाने के लिए डिजिटल प्रमाणपत्र का उपयोग करती हैं।

Feature	Digital Signature	Digital Certificate
Basics / Definition	A digital signature secures the integrity of a digital document in a similar way as a fingerprint or attachment.	Digital certificate is a file that ensures holder's identity and provides security.
Process / Steps	Hashed value of original data is encrypted using sender's private key to generate the digital signature.	It is generated by CA (Certifying Authority) that involves four steps: Key Generation, Registration, Verification, Creation.
Security Services	**Authenticity** of Sender, **integrity** of the document and **non-repudiation**.	It provides security and **authenticity** of certificate holder.
Standard	It follows Digital Signature Standard (DSS).	It follows X.509 Standard Format

Encryption: Process of converting electronic data into another form, called ciphertext, which cannot be easily understood by anyone except the authorized parties. This assures data security.

Decryption: Process of translating code to data.

- The message is encrypted at the sender's side using various encryption algorithms and decrypted at the receiver's end with the help of the decryption algorithms.
- When some message is to be kept secure like username, password, etc., encryption and decryption techniques are used to assure data security.

एन्क्रिप्शन: इलेक्ट्रॉनिक डेटा को सिफरटेक्स्ट नामक एक अन्य रूप में परिवर्तित करने की प्रक्रिया, जिसे अधिकृत पक्षों के अलावा कोई भी आसानी से नहीं समझ सकता। यह डेटा सुरक्षा सुनिश्चित करता है।

डिक्रिप्शन: कोड को डेटा में बदलने की प्रक्रिया।

● संदेश को विभिन्न एन्क्रिप्शन एल्गोरिदम का उपयोग करके प्रेषक की ओर से एन्क्रिप्ट किया जाता है और डिक्रिप्शन एल्गोरिदम की सहायता से प्राप्तकर्ता की ओर से डिक्रिप्ट किया जाता है।

● जब किसी संदेश को सुरक्षित रखना होता है, जैसे उपयोगकर्ता नाम, पासवर्ड, आदि, तो डेटा सुरक्षा सुनिश्चित करने के लिए एन्क्रिप्शन और डिक्रिप्शन तकनीकों का उपयोग किया जाता है।

Types of Encryption

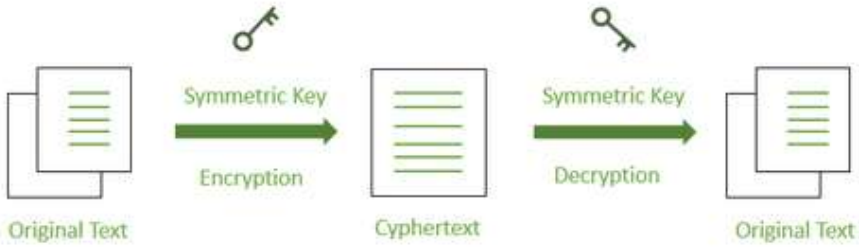
Data encryption transforms information into a code that is only accessible to those with a password or secret key, sometimes referred to as a decryption key. Data that has not been encrypted is referred to as plaintext, whereas data that has been encrypted is referred to as ciphertext. In today's business sector, encryption is one of the most popular and effective data protection solutions. By converting data into ciphertext, which can only be decoded with a special decryption key generated either before or at the time of the encryption, data encryption serves to protect the secrecy of data.

डेटा एन्क्रिप्शन जानकारी को एक कोड में बदल देता है जो केवल पासवर्ड या गुप्त कुंजी वाले लोगों के लिए ही सुलभ होता है, जिसे कभी-कभी डिक्रिप्शन कुंजी भी कहा जाता है। जिस डेटा को एन्क्रिप्ट नहीं किया गया है उसे प्लेनटेक्स्ट कहा जाता है, जबकि एन्क्रिप्ट किए गए डेटा को सिफरटेक्स्ट कहा जाता है। आज के व्यावसायिक क्षेत्र में, एन्क्रिप्शन सबसे लोकप्रिय और प्रभावी डेटा सुरक्षा समाधानों में से एक है। डेटा को सिफरटेक्स्ट में परिवर्तित करके, जिसे केवल एन्क्रिप्शन से पहले या एन्क्रिप्शन के समय उत्पन्न एक विशेष डिक्रिप्शन कुंजी द्वारा ही डिकोड किया जा सकता है, डेटा एन्क्रिप्शन डेटा की गोपनीयता की रक्षा करता है।

- **Symmetric Encryption**
  Data is encrypted using a key and the decryption is also done using the same key. There are a few strategies used in cryptography algorithms. For encryption and decryption processes, some algorithms employ a unique key. In such operations, the unique key must be secured since the system or person who knows the key has complete authentication to decode the message for reading.

- सममित एन्क्रिप्शन

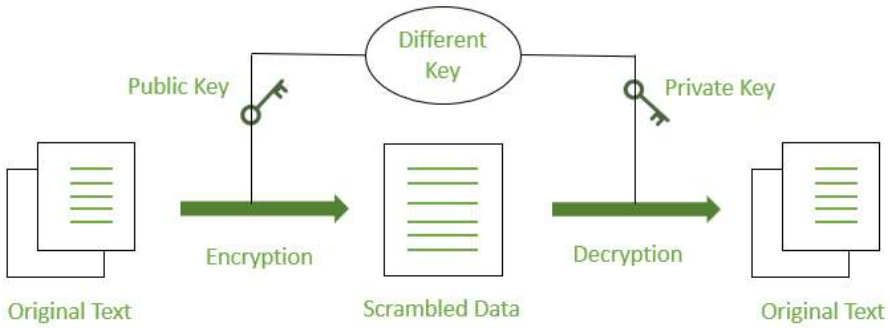
डेटा को एक कुंजी का उपयोग करके एन्क्रिप्ट किया जाता है और डिक्रिप्शन भी उसी कुंजी का उपयोग करके किया जाता है। क्रिप्टोग्राफी एल्गोरिदम में कुछ रणनीतियाँ उपयोग की जाती हैं। एन्क्रिप्शन और डिक्रिप्शन प्रक्रियाओं के लिए, कुछ एल्गोरिदम एक अद्वितीय कुंजी का उपयोग करते हैं। ऐसे कार्यों में, अद्वितीय कुंजी सुरक्षित होनी चाहिए क्योंकि सिस्टम या कुंजी जानने वाले व्यक्ति के पास संदेश को पढ़ने के लिए डिकोड करने हेतु पूर्ण प्रमाणीकरण होता है।



- **Asymmetric Encryption**
  Asymmetric Cryptography is also known as public-key cryptography. It uses public and private keys for the encryption and decryption of message. One key in the pair which can be shared with everyone is called the public key. The other key in the pair which is kept secret and is only known by the owner is called the private key.

● असममित एन्क्रिप्शन

असममित क्रिप्टोग्राफी को सार्वजनिक-कुंजी क्रिप्टोग्राफी भी कहा जाता है। यह संदेश के एन्क्रिप्शन और डिक्रिप्शन के लिए सार्वजनिक और निजी कुंजियों का उपयोग करती है। इस जोड़ी में एक कुंजी जिसे सभी के साथ साझा किया जा सकता है, सार्वजनिक कुंजी कहलाती है। इस जोड़ी में दूसरी कुंजी, जिसे गुप्त रखा जाता है और केवल स्वामी ही जानता है, निजी कुंजी कहलाती है।



1. Public key: Key which is known to everyone. Ex-public key of A is 7, this information is known to everyone.

2. Private key: Key which is only known to the person who's private key it is.

3. Authentication: Authentication is any process by which a system verifies the identity of a user who wishes to access it.

4. Non-repudiation: Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

5. Integrity: To ensure that the message was not altered during the transmission.

6. Message digest: The representation of text in the form of a single string of digits, created using a formula called a one way hash function. Encrypting a message digest with a private key creates a digital signature which is an electronic means of authentication.

1. सार्वजनिक कुंजी: वह कुंजी जो सभी को ज्ञात हो। A की पूर्व-सार्वजनिक कुंजी 7 है, यह जानकारी सभी को ज्ञात है।

2. निजी कुंजी: वह कुंजी जो केवल उसी व्यक्ति को ज्ञात होती है जिसकी वह निजी कुंजी है।

3. प्रमाणीकरण: प्रमाणीकरण वह प्रक्रिया है जिसके द्वारा कोई सिस्टम उस उपयोगकर्ता की पहचान सत्यापित करता है जो उस तक पहुँच प्राप्त करना चाहता है।

4. अस्वीकृति न होना: अस्वीकृति न होना यह सुनिश्चित करने का एक तरीका है कि संदेश भेजने वाला बाद में संदेश भेजने से इनकार नहीं कर सकता और प्राप्तकर्ता संदेश प्राप्त करने से इनकार नहीं कर सकता।

5. अखंडता: यह सुनिश्चित करने के लिए कि प्रेषण के दौरान संदेश में कोई बदलाव नहीं किया गया है।

6. संदेश डाइजेस्ट: अंकों की एकल स्ट्रिंग के रूप में पाठ का निरूपण, जिसे वन-वे हैश फ़ंक्शन नामक सूत्र का उपयोग करके बनाया जाता है। निजी कुंजी के साथ संदेश डाइजेस्ट को एन्क्रिप्ट करने से एक डिजिटल हस्ताक्षर बनता है जो प्रमाणीकरण का एक इलेक्ट्रॉनिक माध्यम है।

DUTIES OF SUBSCRIBER:-

A subscriber is an individual who has signed up for a service, program, or publication that requires regular payment, such as a magazine, newspaper, or internet service.

Under the Indian Information Technology (IT) Act, 2000, subscribers' key duties include generating their own private and public key pairs, accepting digital signature certificates and verifying their content, and, most importantly, exercising reasonable care to retain control of their private key. Subscribers must take all necessary steps to prevent their private key from being disclosed to an unauthorized person and must immediately notify the Certifying Authority (CA) if their private key is compromised.

सब्सक्राइबर वह व्यक्ति होता है जिसने किसी ऐसी सेवा, कार्यक्रम या प्रकाशन के लिए साइन अप किया है जिसके लिए नियमित भुगतान की आवश्यकता होती है, जैसे कि कोई पत्रिका, समाचार पत्र या इंटरनेट सेवा।
भारतीय सूचना प्रौद्योगिकी (आईटी) अधिनियम, 2000 के तहत, सब्सक्राइबर के प्रमुख कर्तव्यों में अपनी निजी और सार्वजनिक कुंजी युग्म बनाना, डिजिटल हस्ताक्षर प्रमाणपत्र स्वीकार करना और

अपनी सामग्री का सत्यापन करना, और सबसे महत्वपूर्ण बात, अपनी निजी कुंजी पर नियंत्रण बनाए रखने के लिए उचित सावधानी बरतना शामिल है। सब्सक्राइबरों को अपनी निजी कुंजी को किसी अनधिकृत व्यक्ति के सामने प्रकट होने से रोकने के लिए सभी आवश्यक कदम उठाने चाहिए और यदि उनकी निजी कुंजी से छेड़छाड़ की जाती है, तो उन्हें तुरंत प्रमाणन प्राधिकरण (सीए) को सूचित करना चाहिए।

The duties of a subscriber typically involve fulfilling their financial obligations and complying with the terms and conditions of the agreement.

एक ग्राहक के कर्तव्यों में आम तौर पर अपने वित्तीय दायित्वों को पूरा करना और समझौते की शर्तों का पालन करना शामिल होता है।

1. **Paying for the Service**: The primary duty of a subscriber is to pay for the service or product they have subscribed to on time. A subscriber must ensure that they pay the subscription fee at the agreed-upon intervals, as failure to do so may result in their account being suspended or canceled.

   सेवा के लिए भुगतान: ग्राहक का प्राथमिक कर्तव्य उस सेवा या उत्पाद का भुगतान समय पर करना है जिसकी उसने सदस्यता ली है। ग्राहक को यह सुनिश्चित करना होगा कि वह तय समय पर सदस्यता शुल्क का भुगतान करे, क्योंकि ऐसा न करने पर उसका खाता निलंबित या रद्द किया जा सकता है।

2. **Following the Terms and Conditions:** A subscriber must abide by the terms and conditions of the subscription agreement. This includes following any rules or regulations regarding the use of the product or service, as well as any restrictions on sharing or distributing content.

   नियम और शर्तों का पालन: ग्राहक को सदस्यता समझौते के नियमों और शर्तों का पालन करना होगा। इसमें उत्पाद या सेवा के उपयोग से संबंधित किसी भी नियम या विनियम का पालन, साथ ही सामग्री के साझाकरण या वितरण पर किसी भी प्रतिबंध का पालन शामिल है।

3. **Providing Accurate Information:** Subscribers must provide accurate and up-to-date information when subscribing to a service. This includes providing correct billing information, contact details, and other relevant information required by the service provider.

   सटीक जानकारी प्रदान करना: किसी सेवा की सदस्यता लेते समय ग्राहकों को सटीक और अद्यतन जानकारी प्रदान करनी होगी। इसमें सही बिलिंग जानकारी, संपर्क विवरण और सेवा प्रदाता द्वारा आवश्यक अन्य प्रासंगिक जानकारी प्रदान करना शामिल है।

4. **Informing the Service Provider of Changes**: Subscribers are responsible for informing the service provider of any changes to their contact information or billing details. This ensures that the service provider can continue to deliver the product or service without interruption.

सेवा प्रदाता को परिवर्तनों की सूचना देना: ग्राहक अपनी संपर्क जानकारी या बिलिंग विवरण में किसी भी परिवर्तन की सूचना सेवा प्रदाता को देने के लिए ज़िम्मेदार हैं। इससे यह सुनिश्चित होता है कि सेवा प्रदाता बिना किसी रुकावट के उत्पाद या सेवा प्रदान करता रहे।

5. **Respecting Intellectual Property Rights:** Subscribers must respect the intellectual property rights of the service provider and any other parties involved. This includes not sharing or distributing copyrighted materials without permission, and not using the service for illegal activities.
बौद्धिक संपदा अधिकारों का सम्मान: ग्राहकों को सेवा प्रदाता और उससे जुड़े किसी भी अन्य पक्ष के बौद्धिक संपदा अधिकारों का सम्मान करना चाहिए। इसमें बिना अनुमति के कॉपीराइट सामग्री को साझा या वितरित नहीं करना, और सेवा का उपयोग अवैध गतिविधियों के लिए नहीं करना शामिल है।

6. **Providing Feedback**: Subscribers can provide feedback on the service or product they have subscribed to. This feedback can be used by the service provider to improve their offerings and provide a better experience for their subscribers.
फ़ीडबैक प्रदान करना: सब्सक्राइबर जिस सेवा या उत्पाद की सदस्यता लेते हैं, उसके बारे में फ़ीडबैक दे सकते हैं। इस फ़ीडबैक का उपयोग सेवा प्रदाता अपनी सेवाओं को बेहतर बनाने और अपने सब्सक्राइबरों को बेहतर अनुभव प्रदान करने के लिए कर सकते हैं।

Conclusion:

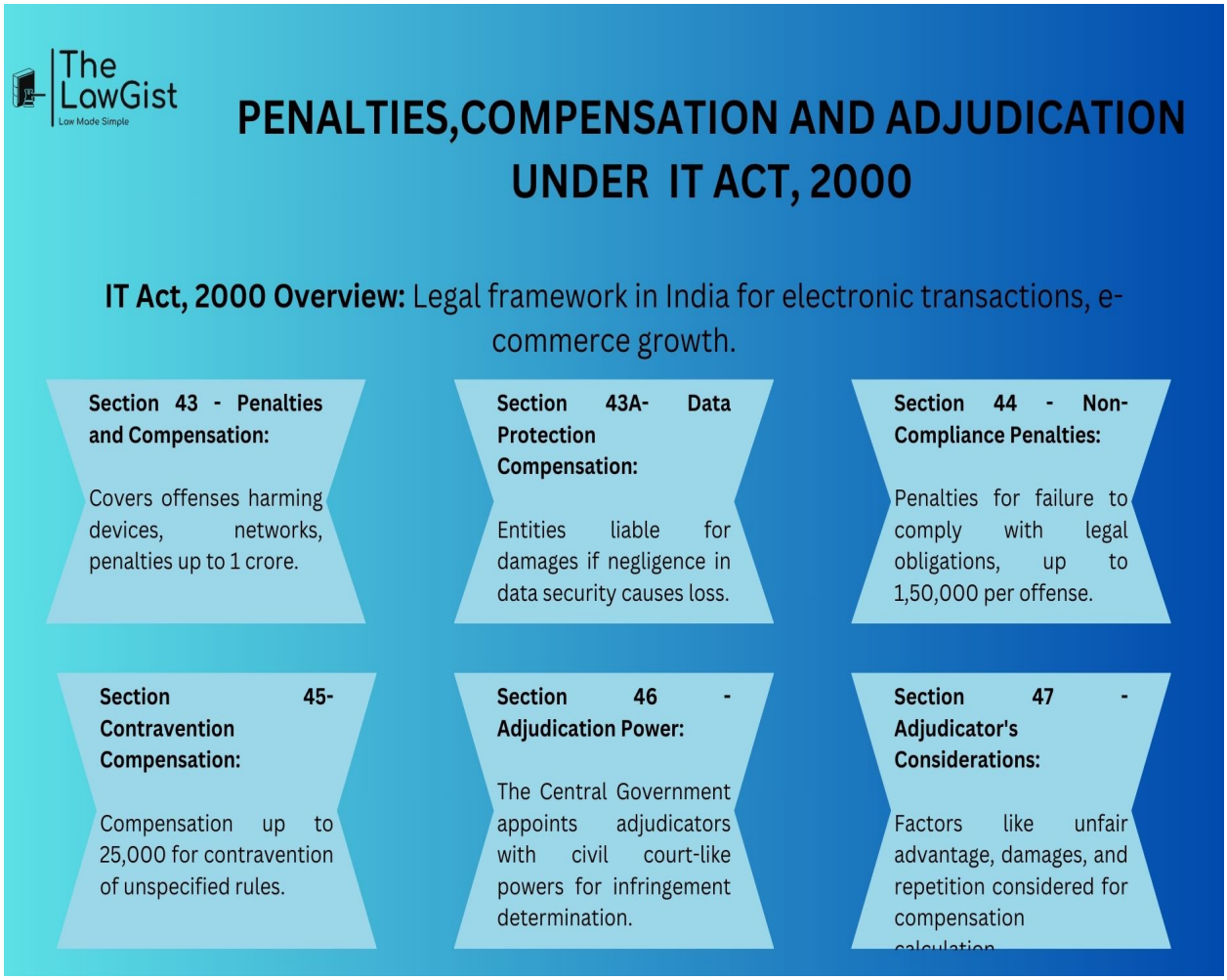
In conclusion, the duties of a subscriber involve fulfilling their financial obligations, complying with the terms and conditions of the agreement, providing accurate information, informing the service provider of any changes, respecting intellectual property rights, and providing feedback. By fulfilling these duties, subscribers can ensure that they receive the service or product they have subscribed to without interruption, while also contributing to the improvement of the service provider's offerings.

संक्षेप में, एक ग्राहक के कर्तव्यों में अपने वित्तीय दायित्वों को पूरा करना, अनुबंध की शर्तों का पालन करना, सटीक जानकारी प्रदान करना, सेवा प्रदाता को किसी भी बदलाव की सूचना देना, बौद्धिक संपदा अधिकारों का सम्मान करना और प्रतिक्रिया प्रदान करना शामिल है। इन कर्तव्यों का पालन करके, ग्राहक यह सुनिश्चित कर सकते हैं कि उन्हें वह सेवा या उत्पाद बिना किसी रुकावट के प्राप्त हो जिसकी उन्होंने सदस्यता ली है, साथ ही सेवा प्रदाता की सेवाओं को बेहतर बनाने में भी योगदान दे सकते हैं।

Penalties and Adjudication

Under the Indian Information Technology (IT) Act, 2000, penalties are levied for contraventions like unauthorized access to computers (Section 43), which can result in civil liability for damages up to ₹1 crore. Criminal offences, such as hacking (Section 66) or publishing obscene material (Section 67), carry imprisonment and fines. Adjudication is the process by which an adjudicating officer, appointed by the government, determines if a contravention has occurred and imposes penalties under Section 46, with the power to act as a civil court.

भारतीय सूचना प्रौद्योगिकी (आईटी) अधिनियम, 2000 के तहत, कंप्यूटर तक अनधिकृत पहुँच (धारा 43) जैसे उल्लंघनों के लिए दंड लगाया जाता है, जिसके परिणामस्वरूप ₹1 करोड़ तक के नुकसान के लिए नागरिक दायित्व हो सकता है। हैकिंग (धारा 66) या अश्लील सामग्री प्रकाशित करने (धारा 67) जैसे आपराधिक अपराधों के लिए कारावास और जुर्माने का प्रावधान है। न्यायनिर्णयन वह प्रक्रिया है जिसके द्वारा सरकार द्वारा नियुक्त एक न्यायनिर्णायक अधिकारी यह निर्धारित करता है कि क्या कोई उल्लंघन हुआ है और धारा 46 के तहत दंड लगाता है, जिसे एक दीवानी न्यायालय के रूप में कार्य करने का अधिकार है।



Introduction

- The IT Act, 2000 regulates cyber activities in India.
- It prescribes **penalties and compensation** for various **civil contraventions** (non-criminal) related to computers, networks, and data.
- Penalties are mainly covered under **Chapter IX (Sections 43 to 47)**.

प्रस्तावना

• आईटी अधिनियम, 2000 भारत में साइबर गतिविधियों को नियंत्रित करता है।

• यह कंप्यूटर, नेटवर्क और डेटा से संबंधित विभिन्न नागरिक उल्लंघनों (गैर-आपराधिक) के लिए दंड और मुआवजे का प्रावधान करता है।

• दंड मुख्य रूप से अध्याय IX (धारा 43 से 47) के अंतर्गत आते हैं।

Penalty and Compensation for Damages (Section 43):

Section 43 of the Information Technology Act, of 2000 delineates penalties and compensations for actions detrimental to devices, computer systems, or computer networks. Offenses include unauthorized access, downloading or copying data without authority, injection of computer contaminants, damages to computer databases, disjuncture of computer systems, denial of access, aiding unauthorized access, charging services to another's account, destruction, deletion, or modification of information, and the stealing, concealing, or damaging of computer source code. The penalties involve compensations not exceeding 1 crore.

सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 43, उपकरणों, कंप्यूटर प्रणालियों या कंप्यूटर नेटवर्क के लिए हानिकारक कार्यों के लिए दंड और क्षतिपूर्ति का निर्धारण करती है। अपराधों में अनधिकृत पहुँच, बिना अनुमति के डेटा डाउनलोड या कॉपी करना, कंप्यूटर दूषित पदार्थों का इंजेक्शन, कंप्यूटर डेटाबेस को नुकसान पहुँचाना, कंप्यूटर प्रणालियों को अलग करना, पहुँच से वंचित करना, अनधिकृत पहुँच में सहायता करना, किसी अन्य के खाते से सेवाओं का शुल्क लेना, सूचना को नष्ट करना, हटाना या संशोधित करना, और कंप्यूटर सोर्स कोड की चोरी, छिपाना या क्षति पहुँचाना शामिल हैं। इन दंडों में 1 करोड़ रुपये से अधिक का मुआवजा शामिल नहीं है।

Compensation for Failure to Protect Data (Section 43A):

Introduced via the Information Technology (Amendment) Act, 2008, Section 43A places liability on entities negligent in maintaining fair security practices. If such negligence causes wrongful loss or benefit to any person due to the mishandling of confidential personal data or information, the entity is liable for damages through compensation.

सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008 के माध्यम से लागू की गई धारा 43A, निष्पक्ष सुरक्षा प्रथाओं को बनाए रखने में लापरवाही बरतने वाली संस्थाओं पर दायित्व डालती है। यदि ऐसी लापरवाही के कारण गोपनीय व्यक्तिगत डेटा या जानकारी के दुरुपयोग के कारण किसी व्यक्ति को अनुचित हानि या लाभ होता है, तो संस्था क्षतिपूर्ति के माध्यम से क्षतिपूर्ति के लिए उत्तरदायी होगी।

Penalty for Failure to Provide Information, Return, or Report (Section 44):

Section 44 of the Information Technology Act,2000 imposes penalties for non-compliance with legal obligations, including failure to submit papers, returns, or reports to the Controller of Certifying Authorities or Certifying Authorities. Failure to provide required documents to the Controller of Certifying Authority may result in penalties:

(a) up to fifteen lakh rupees for each instance,

(b) up to fifty thousand rupees per day for late filing, and

(c) up to one lakh rupees per day for not maintaining necessary books or records.

सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 44, कानूनी दायित्वों का पालन न करने पर दंड लगाती है, जिसमें प्रमाणन प्राधिकरण नियंत्रक या प्रमाणन प्राधिकरणों को कागजात, रिटर्न या रिपोर्ट प्रस्तुत न करना शामिल है। प्रमाणन प्राधिकरण नियंत्रक को आवश्यक दस्तावेज़ उपलब्ध न कराने पर निम्नलिखित दंड लग सकते हैं:

(क) प्रत्येक मामले के लिए पंद्रह लाख रुपये तक,

(ख) देरी से दाखिल करने पर प्रतिदिन पचास हज़ार रुपये तक, और

(ग) आवश्यक बहीखाते या अभिलेख न रखने पर प्रतिदिन एक लाख रुपये तक।

Penalty for Contravention of Rules or Regulations (Section 45):

Section 45 addresses contraventions of rules or regulations specified under the Act. If a person violates such rules, and no penalty is specified, compensation not exceeding 1 lakh rupees may be imposed for the affected person. Additionally, they might be required to compensate the affected party, with amounts capped at ten lakh rupees for intermediaries, companies, or bodies corporate, and one lakh rupees for others.

धारा 45 अधिनियम के तहत निर्दिष्ट नियमों या विनियमों के उल्लंघन से संबंधित है। यदि कोई व्यक्ति ऐसे नियमों का उल्लंघन करता है, और कोई दंड निर्दिष्ट नहीं है, तो प्रभावित व्यक्ति पर अधिकतम 1 लाख रुपये का मुआवज़ा लगाया जा सकता है। इसके अतिरिक्त, उन्हें प्रभावित पक्ष को मुआवज़ा देने की आवश्यकता हो सकती है, जिसकी अधिकतम राशि

मध्यस्थों, कंपनियों या निगमित निकायों के लिए 10 लाख रुपये और अन्य के लिए 1 लाख रुपये तक हो सकती है।

Power to Adjudicate (Section 46):

Section 46 grants the Central Government the authority to appoint an adjudicator, typically an officer of the Government, to determine if a person has committed an infringement and is liable for penalty or compensation. The adjudicator, possessing expertise in information technology and legal matters, has powers akin to a civil court. The section also defines the jurisdiction of adjudicators and outlines their powers and procedures.

धारा 46 केंद्र सरकार को एक निर्णायक, आमतौर पर सरकार का एक अधिकारी, नियुक्त करने का अधिकार देती है ताकि यह निर्धारित किया जा सके कि किसी व्यक्ति ने उल्लंघन किया है और क्या वह दंड या मुआवजे के लिए उत्तरदायी है। सूचना प्रौद्योगिकी और कानूनी मामलों में विशेषज्ञता रखने वाले निर्णायक के पास सिविल न्यायालय के समान शक्तियाँ होती हैं। यह धारा निर्णायकों के अधिकार क्षेत्र को भी परिभाषित करती है और उनकी शक्तियों और प्रक्रियाओं की रूपरेखा प्रस्तुत करती है।

Factors Considered in Penalty (Section 47)

While deciding penalty or compensation, AO considers:

1. **Gain to the offender**
2. **Loss to the victim**
3. **Repeat nature of the default**

दंड या मुआवजे का निर्णय करते समय, एओ निम्नलिखित बातों पर विचार करता है:

1. अपराधी को लाभ
2. पीड़ित को हानि
3. चूक की पुनरावृत्ति

Examples and Analysis:

- **Example**: An employee of a software company gains unauthorized access to the company's database and steals sensitive customer information, including credit card details. The employee then sells this information to a third party for personal gain.

उदाहरण: एक सॉफ्टवेयर कंपनी का एक कर्मचारी कंपनी के डेटाबेस तक अनधिकृत पहुँच प्राप्त कर लेता है और ग्राहकों की संवेदनशील जानकारी, जिसमें क्रेडिट कार्ड विवरण भी शामिल है, चुरा लेता है। फिर वह कर्मचारी निजी लाभ के लिए यह जानकारी किसी तीसरे पक्ष को बेच देता है।

- **Analysis:** The IT Act imposes penalties for unauthorized access and data disclosure, with fines respectively. Victims can seek compensation under Section 43A, and disputes can be adjudicated by the Cyber Appellate Tribunal or relevant authority. This legal framework aims to protect individuals and companies from cybercrimes and ensure accountability for wrongful actions.

विश्लेषण: आईटी अधिनियम अनधिकृत पहुँच और डेटा प्रकटीकरण के लिए क्रमशः जुर्माने का प्रावधान करता है। पीड़ित धारा 43ए के तहत मुआवज़ा मांग सकते हैं, और विवादों का निपटारा साइबर अपीलीय न्यायाधिकरण या संबंधित प्राधिकारी द्वारा किया जा सकता है। इस कानूनी ढाँचे का उद्देश्य व्यक्तियों और कंपनियों को साइबर अपराधों से बचाना और गलत कार्यों के लिए जवाबदेही सुनिश्चित करना है।

Appellate Tribunal

The Cyber Appellate Tribunal (CAT) was established under Section 48 of the Information Technology Act, 2000 (India), to hear appeals against orders issued by adjudicating officers and the Controller of Certifying Authorities under the Act. However, the provisions for the CAT were merged with the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) in 2017, making TDSAT the authority to hear such appeals under the IT Act.

सूचना प्रौद्योगिकी अधिनियम, 2000 (भारत) की धारा 48 के अंतर्गत साइबर अपीलीय न्यायाधिकरण (कैट) की स्थापना, अधिनियम के अंतर्गत निर्णायक अधिकारियों और प्रमाणन प्राधिकरण नियंत्रक द्वारा जारी आदेशों के विरुद्ध अपीलों की सुनवाई हेतु की गई थी। हालाँकि, कैट के प्रावधानों को 2017 में दूरसंचार विवाद निपटान एवं अपीलीय न्यायाधिकरण (टीडीसैट) में मिला दिया गया, जिससे टीडीसैट को आईटी अधिनियम के अंतर्गत ऐसी अपीलों की सुनवाई करने का अधिकार प्राप्त हो गया।

Introduction to Cyber Appellate Tribunal

The Cyber Appellate Tribunal (CAT) stands as a critical institution in the legal landscape. . Established under the Information Technology Act of 2000, the CAT serves as a specialized forum for settling cyber-related disputes, ensuring that citizens have access to fair and impartial proceedings. It defends the rights of individuals and businesses in the online world. The CAT operates independently and has the authority to summon and examine witnesses, require the production of relevant documents, and make decisions based on the principles of natural justice.

साइबर अपीलीय न्यायाधिकरण (कैट) कानूनी परिदृश्य में एक महत्वपूर्ण संस्था है। सूचना प्रौद्योगिकी अधिनियम, 2000 के तहत स्थापित, कैट साइबर संबंधी विवादों के निपटारे के लिए एक विशेष मंच के रूप में कार्य करता है और यह सुनिश्चित करता है कि नागरिकों को निष्पक्ष और निष्पक्ष कार्यवाही तक पहुँच प्राप्त हो। यह ऑनलाइन दुनिया में व्यक्तियों और व्यवसायों के अधिकारों की रक्षा करता है। कैट स्वतंत्र रूप से कार्य करता है और गवाहों को बुलाने और उनसे पूछताछ करने, प्रासंगिक दस्तावेज़ प्रस्तुत करने की माँग करने और प्राकृतिक न्याय के सिद्धांतों के आधार पर निर्णय लेने का अधिकार रखता है।

Establishment of Cyber Appellate Tribunal

The establishment of the Cyber Appellate Tribunal (CAT) was an important moment in India's legal landscape. It was introduced under Section 48 of the Information Technology (Amendment) Act of 2006, which sought to address the unique challenges brought about by the digital age. This move was essential because, as the internet grew, so did the risks associated with it.

In section 48, there are the following sub-sections:

1. The central government shall, by notification, establish one or more appellate tribunals to be known as the cyber appellate tribunal.
2. The central government shall also specify, in the notification referred to in subsection (1), the matters and places in relation to which the cyber appellate tribunal may exercise jurisdiction.

साइबर अपीलीय न्यायाधिकरण (कैट) की स्थापना भारत के कानूनी परिदृश्य में एक महत्वपूर्ण क्षण था। इसे सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2006 की धारा 48 के अंतर्गत प्रस्तुत किया गया था, जिसका उद्देश्य डिजिटल युग द्वारा उत्पन्न विशिष्ट चुनौतियों का समाधान करना था। यह कदम इसलिए आवश्यक था क्योंकि जैसे-जैसे इंटरनेट का विकास हुआ, वैसे-वैसे इससे जुड़े जोखिम भी बढ़ते गए।

धारा 48 में निम्नलिखित उप-धाराएँ हैं:

1. केंद्र सरकार, अधिसूचना द्वारा, एक या एक से अधिक अपीलीय न्यायाधिकरणों की स्थापना करेगी जिन्हें साइबर अपीलीय न्यायाधिकरण के रूप में जाना जाएगा।

2. केंद्र सरकार उपधारा (1) में निर्दिष्ट अधिसूचना में उन मामलों और स्थानों को भी निर्दिष्ट करेगी जिनके संबंध में साइबर अपीलीय न्यायाधिकरण क्षेत्राधिकार का प्रयोग कर सकता है।

Staff of the Cyber Appellate Tribunal

The central government appoints the members of the CAT by notification in the Official Gazette. The members of the CAT are appointed for a period of three years, but they are eligible for reappointment. These individuals work under the direction of the chairperson. The central government sets the salaries, allowances, and other service conditions. This ensures a well-organized and regulated work environment at the cyber appellate tribunal, promoting effective operations and fair treatment of the staff.

केंद्र सरकार आधिकारिक राजपत्र में अधिसूचना द्वारा कैट के सदस्यों की नियुक्ति करती है। कैट के सदस्यों की नियुक्ति तीन वर्ष की अवधि के लिए होती है, लेकिन वे पुनर्नियुक्ति के पात्र होते हैं। ये सदस्य अध्यक्ष के निर्देशन में कार्य करते हैं। केंद्र सरकार वेतन, भत्ते और अन्य सेवा शर्तें निर्धारित करती है। इससे साइबर अपीलीय न्यायाधिकरण में एक सुव्यवस्थित और विनियमित कार्य वातावरण सुनिश्चित होता है, जिससे प्रभावी संचालन और कर्मचारियों के साथ निष्पक्ष व्यवहार को बढ़ावा मिलता है।

Composition of the Cyber Appellate Tribunal

The composition of the Cyber Appellate Tribunal (CAT) is a key aspect that sets it apart from other legal bodies. It reflects a deep understanding of the complexity of cyber-related issues and the necessity for expertise in various domains.

The CAT is headed by a chairperson, who is typically a retired judge from the Supreme Court or a High Court.

In addition to the chairperson, the CAT includes expert members who possess knowledge in fields such as information technology, cybersecurity, and law. These experts act as the backbone of the tribunal, bringing technical insight and specialized legal expertise to the table.

Think of the CAT's composition as a team of both seasoned players and fresh talent. The combination of legal wisdom and technical know-how ensures that the CAT is well-equipped to comprehend and address even the most intricate cyber-related cases. This diverse composition ensures that justice is served fairly in the digital world.

साइबर अपीलीय न्यायाधिकरण (कैट) की संरचना एक महत्वपूर्ण पहलू है जो इसे अन्य कानूनी निकायों से अलग करती है। यह साइबर-संबंधी मुद्दों की जटिलता और विभिन्न क्षेत्रों में विशेषज्ञता की आवश्यकता की गहरी समझ को दर्शाता है।
कैट का नेतृत्व एक अध्यक्ष करता है, जो आमतौर पर सर्वोच्च न्यायालय या उच्च न्यायालय का सेवानिवृत्त न्यायाधीश होता है।

अध्यक्ष के अलावा, कैट में सूचना प्रौद्योगिकी, साइबर सुरक्षा और कानून जैसे क्षेत्रों का ज्ञान रखने वाले विशेषज्ञ सदस्य भी शामिल होते हैं। ये विशेषज्ञ न्यायाधिकरण की रीढ़ की हड्डी के रूप में कार्य करते हैं, तकनीकी अंतर्दृष्टि और विशिष्ट कानूनी विशेषज्ञता प्रदान करते हैं। कैट की संरचना को अनुभवी और नई प्रतिभाओं, दोनों की एक टीम के रूप में देखें। कानूनी ज्ञान और तकनीकी जानकारी का संयोजन यह सुनिश्चित करता है कि कैट सबसे जटिल साइबर-संबंधी मामलों को भी समझने और उनका समाधान करने के लिए पूरी तरह से सुसज्जित है। यह विविध संरचना यह सुनिश्चित करती है कि डिजिटल दुनिया में न्याय निष्पक्ष रूप से प्रदान किया जाए।

Limitations of the CAT

The limitation of the CAT is related to tribunal appeals. Section 61 of the Information Technology Act, 2000 states that regular courts cannot handle cases related to matters that the cyber appellate tribunal is authorized to decide. So, if you have an issue that the CAT can address, you cannot take it to a civil court. Instead, you must begin by filing an appeal with the CAT. The CAT is a specialized tribunal with expertise in information technology law, essential for resolving issues in the digital world. Also, it is faster and more cost-effective than civil courts, which can be slow, expensive, and lack the necessary expertise for digital disputes.

कैट की सीमाएँ न्यायाधिकरण की अपीलों से संबंधित हैं। सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 61 के अनुसार, नियमित अदालतें उन मामलों को नहीं संभाल सकतीं जिन पर निर्णय लेने का अधिकार साइबर अपीलीय न्यायाधिकरण को है। इसलिए, यदि आपके पास कोई ऐसा मुद्दा है जिसका समाधान कैट कर सकता है, तो आप उसे दीवानी अदालत में नहीं ले जा सकते। इसके बजाय, आपको कैट में अपील दायर करके शुरुआत करनी होगी।

कैट एक विशिष्ट न्यायाधिकरण है जो सूचना प्रौद्योगिकी कानून में विशेषज्ञता रखता है, जो डिजिटल दुनिया में समस्याओं के समाधान के लिए आवश्यक है। साथ ही, यह दीवानी अदालतों की तुलना में तेज़ और अधिक लागत प्रभावी है, जो धीमी, महंगी हो सकती हैं और जिनमें डिजिटल विवादों के लिए आवश्यक विशेषज्ञता का अभाव होता है।

Offences And Cyber Crimes

Offences under India's IT Act 2000 include computer-related offenses like hacking, data theft, and unauthorized access, as well as offenses related to publishing obscene material, identity theft, and cyber terrorism. The Act also covers offenses like cheating by personation, violation of privacy, and publishing sexually explicit material without consent. Penalties can include fines and imprisonment, with severe punishments like life imprisonment for cyber terrorism.

भारत के आईटी अधिनियम 2000 के तहत अपराधों में कंप्यूटर से संबंधित अपराध जैसे हैकिंग, डेटा चोरी और अनधिकृत पहुँच, साथ ही अश्लील सामग्री प्रकाशित करने, पहचान की चोरी और साइबर आतंकवाद से संबंधित अपराध शामिल हैं। यह अधिनियम छद्म रूप में धोखाधड़ी, निजता का उल्लंघन और बिना सहमति के यौन सामग्री प्रकाशित करने जैसे अपराधों को भी कवर करता है। दंड में जुर्माना और कारावास शामिल हो सकते हैं, साइबर आतंकवाद के लिए आजीवन कारावास जैसी कठोर सजाएँ भी हो सकती हैं।

Computer-Related Offences

- **Unauthorized Access:** Accessing a computer system without permission.
- **Hacking:** Tampering with or gaining unauthorized entry into computer systems.
- **Data Diddling/Theft:** Illegally copying, downloading, or stealing information from a system.
- **Virus/Worm Introduction:** Introducing malicious software into computer systems.
- **Denial-of-Service Attacks:** Disrupting a computer system or denying authorized users access to it.
- **Logic Bombs & Trojan Attacks:** Using malicious software to cause harm to systems.

• अनधिकृत पहुँच: बिना अनुमति के कंप्यूटर सिस्टम तक पहुँचना।
• हैकिंग: कंप्यूटर सिस्टम के साथ छेड़छाड़ करना या उसमें अनधिकृत रूप से प्रवेश करना।
• डेटा हेराफेरी/चोरी: सिस्टम से अवैध रूप से जानकारी की नकल करना, डाउनलोड करना या चोरी करना।
• वायरस/वर्म का परिचय: कंप्यूटर सिस्टम में दुर्भावनापूर्ण सॉफ़्टवेयर डालना।
• सेवा निषेध हमले: कंप्यूटर सिस्टम को बाधित करना या अधिकृत उपयोगकर्ताओं को उस तक पहुँच से वंचित करना।
• लॉजिक बम और ट्रोजन हमले: सिस्टम को नुकसान पहुँचाने के लिए दुर्भावनापूर्ण सॉफ़्टवेयर का उपयोग करना।

Cyber Crime

Cyber Crime is not defined officially in IT Act or in any other legislation. In fact, it cannot be too. Offence or crime has been dealt with elaborately listing various acts and the punishments for each, under the Indian Penal Code, 1860 and related legislations. Hence, the concept of cyber crime is just a “combination of crime and computer”.

Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

Any contract for the sale or conveyance of immovable property or any interest in such property; Any such class of documents or transactions as may be notified by the Central Government

आईटी अधिनियम या किसी अन्य कानून में साइबर अपराध को आधिकारिक रूप से परिभाषित नहीं किया गया है। वास्तव में, इसे परिभाषित भी नहीं किया जा सकता। भारतीय दंड संहिता, 1860 और संबंधित कानूनों के तहत, अपराध या अपराध को विभिन्न कृत्यों और प्रत्येक के लिए दंडों को विस्तृत रूप से सूचीबद्ध करके परिभाषित किया गया है। इसलिए, साइबर अपराध की अवधारणा केवल "अपराध और कंप्यूटर का संयोजन" है।
संकीर्ण अर्थ में साइबर अपराध (कंप्यूटर अपराध): इलेक्ट्रॉनिक संचालन के माध्यम से निर्देशित कोई भी अवैध व्यवहार जो कंप्यूटर सिस्टम और उनके द्वारा संसाधित डेटा की सुरक्षा को लक्षित करता है।
व्यापक अर्थ में साइबर अपराध (कंप्यूटर से संबंधित अपराध): कंप्यूटर सिस्टम या नेटवर्क के माध्यम से या उसके संबंध में किया गया कोई भी अवैध व्यवहार, जिसमें कंप्यूटर सिस्टम या नेटवर्क के माध्यम से अवैध रूप से जानकारी रखना, पेश करना या वितरित करना जैसे अपराध शामिल हैं।
अचल संपत्ति की बिक्री या हस्तांतरण के लिए कोई अनुबंध या ऐसी संपत्ति में कोई हित; दस्तावेज़ों या लेन-देनों का कोई भी ऐसा वर्ग जिसे केंद्र सरकार द्वारा अधिसूचित किया जा सकता है

Other Cyber Crimes

- **Publishing Obscene Material:**
  Section 67 of the IT Act criminalizes the publication or transmission of obscene content in electronic form.
- **Transmitting Sexually Explicit Material:**
  Section 67A punishes the publishing or transmitting of content containing sexually explicit acts.
- **Child Pornography:**
  Section 67B addresses the transmission of material that depicts children in a sexually explicit manner.
- **Violation of Privacy:**
  Section 66E deals with the violation of privacy, such as the intentional capture, publication, or transmission of images of a person's private parts without consent.
- **Identity Theft:**
  Section 66C punishes individuals who fraudulently use another person's identity.
- **Cheating by Personation:**
  Section 66D addresses cheating by falsely pretending to be someone else.
- **Cyber Terrorism:**
  Section 66F criminalizes acts that threaten India's unity, integrity, security, or sovereignty by disrupting critical infrastructure or causing injury to persons or property.

• अश्लील सामग्री प्रकाशित करना:

आईटी अधिनियम की धारा 67 इलेक्ट्रॉनिक रूप में अश्लील सामग्री के प्रकाशन या प्रसारण को अपराध मानती है।

• यौन रूप से स्पष्ट सामग्री प्रसारित करना:

धारा 67A यौन रूप से स्पष्ट कृत्यों वाली सामग्री के प्रकाशन या प्रसारण को दंडित करती है।

• बाल पोर्नोग्राफ़ी:

धारा 67B ऐसी सामग्री के प्रसारण को संबोधित करती है जिसमें बच्चों को यौन रूप से स्पष्ट रूप से दर्शाया गया हो।

• गोपनीयता का उल्लंघन:

धारा 66E गोपनीयता के उल्लंघन से संबंधित है, जैसे कि किसी व्यक्ति की सहमति के बिना उसके गुप्तांगों की जानबूझकर तस्वीरें लेना, प्रकाशित करना या प्रसारित करना।

• पहचान की चोरी:

धारा 66C उन व्यक्तियों को दंडित करती है जो धोखे से किसी अन्य व्यक्ति की पहचान का उपयोग करते हैं।

• छद्म रूप धारण करके धोखाधड़ी:

धारा 66D किसी और के होने का झूठा दिखावा करके धोखाधड़ी को संबोधित करती है।

• साइबर आतंकवाद:

धारा 66F उन कृत्यों को आपराधिक बनाती है जो महत्वपूर्ण बुनियादी ढांचे को बाधित करके या व्यक्तियों या संपत्ति को नुकसान पहुँचाकर भारत की एकता, अखंडता, सुरक्षा या संप्रभुता को खतरा पहुँचाते हैं।