International Journal of Law
ISSN: 2455-2194; Impact Factor: RJIF 5.12
Received: 23-12-2020 Accepted: 06-01-2021; Published: 01-02-2021
www.lawjournals.org
Volume 7; Issue 1; 2021; Page No. 93-100

A legal parlance between electronic commerce and the ICT act 2006: Bangladesh perspective

Md Mahfuzur Rahman
Senior Lecturer, Department of Law, North Western University, MA Bari Road, Sonadanga, Khulna, Bangladesh

Abstract
Communication means has distorted to a great extent within the sphere of our habitual life with the advent of technology in this contemporary era. Information with respect to our living is shared through different up to date means. These modern means or technology used to convey information is termed as Information and Communication Technology (ICT) that is strongly associated with internet. Internet has unlocked a new possibility for trade and commerce, which is electronic commerce (E-Commerce). E-Commerce significantly relies on internet for advertisement, identification, payment and delivery of goods. The rapid growth of E-Commerce is a key prospect for domestic and international trade development of Bangladesh. The growth of E-Commerce requires the vibrant and efficient regulatory mechanism to further build up the legal infrastructure which also ensures the successful operation of E-Commerce in Bangladesh. However, all these dogmatic machinery and legal infrastructure works within the realm of virtual world. A number of legal experts consider that legal regulation of the internet is indispensable to ensure the fast growth of technologies and internet and no action on the internet could be examined free from the control of the cyber law because aspects of the internet may cause much debate in the society without any legal safeguard. This study aims to confer different legal instrument of E-Commerce under the ICT Act, 2006 to demonstrate that how E-Commerce is operating with legal safeguard.

Keywords: electronic commerce, legal mechanism, digital signature, asymmetric cryptosystem, electronic evidence, Bangladesh

Introduction

With the inception of internet and its commercialization since in the late of 90s, E-Commerce quickly entered into the new world market. E-commerce may be defined as the use of the internet and other networking technologies for carrying out business transactions. Nowadays most people assume, E-Commerce means online shopping. However, web shopping is only a little component of the whole scenario. In addition, E-Commerce includes business-to-business links that make purchasing easier for giant corporations. In addition, E-Commerce will extensively have impact on the global economy as well as play an imperative part in future economic progress. Several developing countries have started to adopt policies to endow with a consistent legal and regulatory structure to sustain electronic transactions across state, national and international boundaries. Thus, E-Commerce includes several issues with regard to organizational supervision, commercial settlement and contract, legal and regulatory frameworks, financial settlement measures and taxation, among many others. Internet facilitates also includes carrying out of commercial transaction through online [1]. It is fundamentally a business to business or business to consumer or inter-organizational communication. The growth and development in the field of E-Commerce has evenly required efficient regulatory machinery. Cyber law is still a relentlessly growing course of action. With the growth of internet, some issues are also growing relating to jurisdiction, Cyber Crime, acceptability of e-transaction etc. Electronic Commerce (EC)/Electronic Data Interchange (EDI) has made the way more easier for people to stare at commercial and managerial interactions of information because it works without paper. In the world of paper documents, the established norms of contract and commercial law have been adequate to resolve legal disputes pertaining to these documents.

However, an EDI imposes new risks and behavior related to legality electronic data interchange transaction, digital signature, and the risk of invalid transmission, lost record, disruption and fraud. These are few complex issues of security, privacy, authentication and anonymity, which have been plunge into the front as confidential information increasingly lying modern networks. For the operation of E-Commerce, confidence, reliability and protection of information against security threats are very crucial prerequisite. A security threat may be defined as a crucial condition or event with the potential to cause economic destitution or loss of data or set of network resources by disclosure, modification of data, defiance of service, fraud, Waste and abuse [2]. Therefore, to secure electronic transaction ICT Act was enacted and it came into force on October 08, 2006. In sum, the fast developing technology modernism in the world of the wireless internet require for growing governance competency among social, educational and political organization to create an equitable and safe knowledge based society.

Meaning and Concept of E-Commerce

Commerce is an unrestrained operation between two parties playing a very common role that is buyer and seller. Somebody must do the selling, somebody must do the buying, and these two bodies must share a basic understanding of how the transaction is generally supposed to flow for successful commercial undertakings. Electronic commerce, usually known as E-Commerce, consists of the exchange of products or services over electronic means such

as the internet and other computer networks. E-Commerce describes the buying, selling, and exchanging of products, services, and information through computer networks, primarily the internet. E-Commerce is varying all efficient trading areas and their vital tasks, covering from advertising to paying bills. In simple terms, E-Commerce is a means of automated buying and selling both by purchaser and from by company, which facilitates choosing the goods, ordering, delivery, after sales support and payment [3].

E-Commerce is an umbrella concept to assimilate a wide range of existing and new applications. The World Trade Organization (WTO) Ministerial Declaration (held on 2013) on E- Commerce defines E-Commerce as the production, distribution, marketing, sales or delivery of goods and services by electronic means. The foremost medium of E-Commerce that have been recognized by WTO are telephone, fax, TV, electronic payment and money transfer system, electronic data interchange (EDI) and the internet [4]. According to European Commission, E-Commerce largely initiates the purchase of goods online. It covers a distinct set of undertakings, such as shopping, browsing the internet for goods and services, assembling information about items to purchase and completing the transaction. It also involves the realization and delivery of those goods and services and inquiries about the status of orders [5]. Like any other persistent business activity is also means conducting consumer satisfaction surveys, capturing information about consumers and maintaining consumer databases for marketing promotions and other related activities. Electronic transactions are theoretically very analogous to conventional (paper-based) commercial transactions. Vendors present their products, prices and terms to potential buyers. Buyers consider their options, settle prices and terms (where possible), place orders and make payment. Then, vendors deliver the purchased products. While the specific order of these procedures and the mechanisms through which they are transacted vary, these activities are in principle, elementary to both traditional and electronic commerce. For example, if any person wants to buy books from online then he has to visit the website of that particular company where the offered books and prices are shown to the customers and after contentment the buyer place order under a unique code or identification number and make payment in cash after delivery or before through a variety of payment method suggested by the company.

Present Scenario of E-Commerce in Bangladesh

In Bangladesh, there is an excessive zeal towards e-business; however, due to various economic, infrastructural and lack of security reasons it has not spread. Most imperative companies, associations, chambers and government offices have set up websites. These sites primarily provide information about the organization, and its products and services. There are a small number of sites where monetary transactions can be completed. Main reasons for low e-commerce transactions are: dearth of legal framework for carrying out an electronic business or financial payment system, low internet usage due to lack of adequate telecom facilities, and on the whole lack of confidence in the security and trustworthiness of e-commerce transactions [6].

Comparatively the online trade industry is getting more extensive as the internet based activity signifies huge business in Bangladesh especially during the Covid-19 pandemic. People have become more fascinated in online shopping for ensuring their health security. Nowadays, government is giving their tiresome effort to lift up the ICT based communication in Bangladesh by legal form and arranging infrastructures.

Dimensions of E-Commerce in Bangladesh

There are three dimensions of E-Commerce in Bangladesh. Such as:

A. Business-to-business e-commerce is conducted between the businesses or among the businesses. Most of B 2 B applications are chosen in the area of allocation management, stock management, channel management, dealer management and payment management [7].
B. Business-to-Consumer ecommerce is concerned about the businesses and the consumers. Most of B 2 C e-commerce deals with purchasing of corporeal goods like books or any consumer product, information goods like software, e-book, games, song etc., and private finance management like e-banking [8].
C. B 2 G is generally linked with licensing process, public purchasing and other government operations. This sort of e-commerce is insignificant in comparison to other kind of e-commerce, but it can play a dynamic undertaking for operating public sectors which is referred as e-governance [9].

Popular E-Commerce Sites

There are five mostly accepted e-Commerce web sites e.g., Daraz.com.bd (https://www.daraz.com.bd/), Ajkerdeal.com (https://ajkerdeal.com/), Bagdoom.com (https://www. bagdoom.com/), Chaldal.com (https://chaldal. com /), Rokomari.com (https://www.rokomari.com/). Despite these there are different e-commerce web sites [10]. in Bangladesh.

The Legal Mechanism as the Lifeblood of E-Commerce in Bangladesh

The E-Commerce clearly relates to buying and selling of goods and services through electronic means especially on the cyber space but E-Commerce cannot be augmented without vibrant and efficient legal mechanism. The crucial role is played in the E-Commerce mechanism as following:

Regulation of Digital Signature and Transaction under the ICT Act, 2006

The ICT Act, 2006 was passed to fulfill the following three objects as stated in the preamble

- Providing legal recognition and safety measures of Information and Communication Technology and to categorize rules of relevant subjects.
- Ensuring the legal security of documentary interactions between persons, partnerships and the States, regardless of the medium used; the reliability of legal rules and their application to documentary communications using media based on information technology, whether electronic, magnetic, optical, wireless or other, or based on an arrangement of technologies.
- Harmonizing the technical systems, norms and Principles involved by means of technology-based documents and interoperability between different media and information technologies.

Aside from the above mentioned objectives, the prime propellant on which the whole structure of the Act is based

that is confidence reposed between business partners. The abuse of confidence must be subject to law. The ICT Act, 2006 was passed to aid electronic commerce and hence, it provides legal recognition to electronic records, to digital signature etc. and also deals with specific method of electronic transactions. Such as:

Asymmetric Cryptography

The word Cryptology stems from Greek root meaning 'hidden word' and is used to express the ancient science of top secret communications. It means a method capable of generating a secure key pair consisting of a private key and public key [11].

This definition pertains to the dual key encryption techniques. Encryption is a technique to translate data into an incomprehensible form that cannot be recovered into the original layout without a secret decryption key. The purpose of applying cryptography to documents to transmit over the open networks, such as the internet, is to put a stop to vital information getting into the hands of illicit persons [12]. There are basically two types of encryptions:

- Symmetric (secret/private) key
- Asymmetric (public) key

This cryptographic method is concentrated with the use of two cryptographic keys: a public key and a private key. The public key is distributed without restraint and made available to anyone who desires to send a message to a given person. Private or Symmetric key creates digital signature and public key verifies the digital signature which is called dual key encryption techniques [13].

The encryption used for these keys is of such a high degree of complexity that it is theoretically not viable to crack within a rational timeframe. Transaction security is a noteworthy difficulty to the expansion of E- Commerce. Parties must be able to use techniques to ensure that the business conducted over the networks will be secure. The most reliable means is through cryptography (i.e. encryption and decryption techniques) [14].

Cryptography uses complicated mathematical algorithms, mostly a technology known as 'Asymmetric Cryptography'. Cryptography can be differentiated between the following [15].

- Use of cryptography for securing the confidentiality of a message and
- Use of cryptography in digital signature.

The most accepted and handy method of encryption for wide-ranging messaging is public key cryptography that is encryption and decryption techniques involve the use of two kinds of keys, public keys and private keys, both of which are mathematically linked. One key is used for encryption and the other subsequent key is used for decryption. Each consumer has a pair of keys, of which the private key is kept undisclosed and the public key is open to all [16].

Adoption of Digital Signature

The term digital signature is defined in section 2(1) of The ICT Act, 2006 as Digital Signature means data in an electronic form, which is related with any other electronic data directly or logically and is able to satisfy the validity of the digital signature by affixing with the signatory uniquely, identifying the signatory using a means under the sole control of the signatory and specifying any alteration made in the data thereafter.

In other way, 'Digital Signature' means a Signature affixed in electronic from consisting of a transformation of an electronic record using asymmetric cryptosystem and a hash function such that a person having the original untransformed electronic record and the signer's public key can truly find out whether the transformation was created using the private key that corresponds to the signer's public key and whether the initial electronic record has been altered since the conversion was made [17].

A digital signature involves two components - the public key and the private key. The sender signs a document using his private key that guarantees the document's protection in transit as the manuscript is encrypted and only the correspondent has access to his private key [18]. The reasons for placing a digital signature on an electronic document are precisely the same as the reasons for placing a handwritten signature on a paper document. Such as:

Identification: By placing a signature on a document, the signer identifies himself by the distinctive style of writing his name. Similarly, a digital signature uniquely identifies the sender of an electronic message [19].

Authentication: Signer acknowledges that he authorizes and adopts the contents of the document with his signature. Similar, intention can be ascribed to the sender of the digitally signed e-mail message [20].

Security: A signature on a document should be difficult to forge. Moreover, some aspect of the signature, such as the individuality of the style of the person signing, offers security to the other party that as to the identity of the signer. Digital signatures offer the same form of security [21].

Tamper Resistance: The character of a written signature is such that changes to the signed content or the signature itself are apparent without a doubt except in the case of the skillful forgeries. A digital signature, if anything, is even more tampering proof as they are almost incapable of being forged without actually altering the message irretrievably [22].

Digital Signature and Public Key Infrastructure Process

The fundamental difficulty related to digital signature management is that it operates in online and software driven space without human intervention. Sender sends a digitally signed message then recipient receives and verifies it. The only requisite is that both sender and the recipient must have digital signature software at their own ends. A digital signature certificate security binds the identity of the subscriber [23]. It represents name of the subscriber, his public key information, name of the certifying authority who granted the digital signature certificate, its public key information and the certificate's legitimacy. These certificates are compiled in an online storage area that is publicly accessible maintained by the Controller of Certifying Authorities or in the repository maintained by the Certifying Authority. Every Certifying Authority (CA) has to retain function as indicated by its certification practice statement (CPS). The Certification Practice Statement (hereinafter referred to as CPS) specifics the practices that each Certifying Authority employs in issuing digital signature certificates [24].

The mass execution of digital signature certificates in the internet atmosphere is prepared via Public Key Infrastructure. It establishes a framework or system to use digital signature certificates, encryption and digital signatures as an authentication mechanism and devises supervision methods for such usage. The indispensable idea at the rear of Public Key Infrastructure (hereinafter referred to as PKI) is to combine the use of digital certificates, CAs and other security mechanisms to endow with an infrastructure that can uniquely validate each party involved in E-Commerce, thereby making E-Commerce more secure [25].

Digital Signature or Electronic Signature Certificate

In simple terms, a digital certificate is a reliable electronic method of signing electronic documents that provides the recipient a path to authenticate the sender and also verify whether the content of the document has been tampered with or not using a method of cryptography called asymmetric encryption. Unlike symmetric encryption, which uses the identical secret password to view messages, asymmetric encryption, also called public key encryption, uses a pair of keys, to be precise a public and a private key.

The ICT Act, 2006 exclusively deals with various legal mechanisms relating to Digital Signature Certificate in the following way:

Issue of Certificate: Under Section 36 the Certifying Authorit [26]. may issue a certificate to a prospective subscriber only after the Certifying Authority received an application in the prescribed form requesting for issuance of a certificate from the prospective subscriber having a certification practice statement complied with all of the practices. The prospective subscriber is to be listed in the certificate to be issued and all information in the certificate to be issued must be correct with the payment of proper fees [27].

Representations upon Issuance of Certificate: Under Section 37 by issuing a certificate, the Certifying Authority represents to any person who reasonably relies on the certificate or digital signature described in the certificate that the Certifying Authority has issued the certificate in accordance with any applicable certification practice statement incorporated by reference in the certificate. But, In the absence of such certification practice statement, the Certifying Authority represents that it has confirmed that the Certifying Authority has complied with all applicable requirements; all information in the certificate is accurate, unless the Certifying Authority has affirmed that the accuracy of precise information is not confirmed; the Certifying Authority has no knowledge of any material fact which if it is incorporated in the certificate would badly affect the trustworthiness of the representations [28].

Revocation of Digital Signature Certificate: A Certifying Authority shall revoke a Digital Signature Certificate issued by it on fulfilling the following conditions:

- Making a request by the subscriber or any person authorized by him.
- On the death of the subscriber.
- If the subscriber is a firm or a company and dissolved or wound up or has otherwise ceased to exist.

Certifying Authority may revoke a Digital Signature Certificate which has been issued by it whenever if it is found that a material fact represented in the Digital Signature Certificate is forged or has been concealed; a prerequisite for issuance of the Digital Signature Certificate was not satisfied; the Certifying Authority's identification/security system was compromised in a manner materially or as a whole affecting the Digital Signature Certificate's reliability; the subscriber has been declared insolvent by a competent court or authority. But, A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter [29].

Suspension of Digital Signature Certificate: The Certifying Authority may suspend Digital Signature Certificate on receipt of an application to that effect from the subscriber listed in the Digital Signature certificate or any person accordingly have authoritative power to act for that subscriber. Certifying Authority may also suspend such Digital Signature Certificate to guarantee public interest and for this 30 days notice must be provided to the subscriber and such suspension becomes absolute after reply upon the Non-Satisfaction of the Certifying Authority. Where a Digital Signature Certificate is revoked or suspended, the Certifying Authority shall publish a notice of such revocation or suspension, in the repository specified in the Digital Signature Certificate for publication of such notice [30].

Regulation of Certifying Authority

The problem of identification of public key holder can be solved by appointing a third party, trusted by sender as well as recipient to perform the tasks necessary to associate a person or entity with a specific public key. This third party is generally called as Certifying Authority and the person to whom the certificate is issued is called subscriber. It is a trusted body either public or private that ascertain the identity of the applicant of digital signature certificate and certifies that the public key of a public-private key pair used to create digital signature belongs to that person. The regulation of Certifying Authorities is primarily done by the Controller of Certification Authorities, who is vested with the functions of licensing, certifying, monitoring and overseeing the activities of Certifying Authorities. The government notified the Certifying Authority Rules (CA Rules) on 13 April 2010, which prescribe the conditions under which Certifying Authority can apply for a license in, and carry on their operations. Chapter-V of The ICT Act, 2006 has adopted mechanism for the registration and operation of the Certifying Authorities. The process of issuing a certificate generally requires [31].

- Public-private key pair to be generated by the applicant.
- Verification of identity such as identity card, driver's license or passport.

The applicant demonstrates that he/she holds the private key corresponding to the public key without disclosing the private key. Once the CA has confirmed the association between an identified person and a public key, the CA then issues a certificate.

Duties of Subscribers

Every certifying authority has certain responsibilities. The

subscribers too have certain duties. Chapter-VII specifies the duties of subscriber. The term "subscriber" is defined in section 2(15) of the ICT Act, 2006 as a person in whose name the digital signature certificate is issued. The ICT Act, 2006 envisages a pair of keys-one private and the other public.

It is the duty of the subscriber to preserve control of his private key corresponding to the public key listed in its digital signature certificate. The subscriber should keep the identity of his digital signature in secret. He solely owes a duty to notify the certifying authorities without any encumbrance in case his private key has been compromised in any manner [32].

A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate to one or more persons or in a repository. By accepting Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that all representations made by the subscriber to the Certifying Authority relevant to the information contained in the Digital Certificate are true and all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true [33].

All material representations made by the subscriber to a Certifying Authority for purposes of obtaining a certificate, including all information known to the subscriber shall be accurate and complete to the best of the subscriber's knowledge and belief. Every subscriber shall exercise reasonable care to retain control of using of Digital Signature Certificate and take all steps to prevent its disclosure and if the security of Digital Signature Certificate has been compromised by disobeying the rules the subscriber shall communicate the same without any delay to the Certifying Authority who has issued the Digital Signature Certificate [34].

Admissibility of Electronic Evidence

The ICT Act, 2006 was enacted on the basis of The United Nation Commission on International Trade Law (hereinafter referred to as UNCITRAL) Model Law of Electronic Commerce 1996 (Model Law) as it includes a provision dealing with admissibility and evidential weight of data messages to conduct business electronically and more efficiently. The expression data messages is defined to include information generated, sent, received or stored by electronic, optical or similar means, including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy [35]. Article 9 of Electronic Commerce 1996 (Model Law), provides that the set of laws of evidence must not contradict the admissibility of a electronic message in evidence only for its nature as it is a data message, nor where the data message is the best evidence rationally admissible, on the grounds that it is not in its original form. Article 9(1) of the UNCITRAL Model law on Electronic Commerce (1996) substantially explains the acceptability and evidentiary value of data messages. The article emphasizes that in any legal proceeding, the set of laws of evidence should not apply to rule out a data message because it is in an electronic figure or, if it is the best evidence that the person adducing it could rationally be anticipated to attain on the argument that it is not in its original form. The Enactment Guide of the UNCITRAL Model Law on Electronic Commerce, as regards Art (9) states, the purpose of.... Art 9(1) is to establish that data messages should not be denied admissibility as evidence in legal proceedings on the sole ground that they are in electronic form; puts emphasis on the general principles stated in Article 4 and is needed to make it expressly applicable to admissibility of evidence [36].

Law of Evidence and Computer Generated Evidence

The law should be indicative of positive acceptance of the use of information technology and dynamism to facilitate its growth. The rise of Computers/Internet has created numerous troubles for the law. Several legal rules extensively emphasize on the existence of paper records, of signed records, of original records. The Law of Evidence traditionally relies on paper records as well though of course oral testimony and other kinds of physical objects have always been part of court-rooms, too. It has become obvious to put emphasis on electronic evidence due to carrying out of legal activities through internet at present times [37]. There has been a growing demand from industry and users for new types of signatures to effectively substitute the hand written signature in the electronic environment, granting integrity, confidentiality and authenticity of information and documents. The advent of the internet is similar to that of the telephone, telegraph, and fax-machine communication is facilitated. The enormous focus on facilitating the speed and use of technology with specific reference to the admissibility of electronic evidence is a must to ensure a proper examination of electronic evidence adduced before the court. The system so devised to encompass technologies. With the enactment of The ICT Act, 2006 the law recognizes electronic counter parts of paper documents and signatures and made admissible before courts. They may be proved with few barriers such as requirements of originals. Thus, electronic records are susceptible to tampering and there is no completely proven way of authentication. However, the acceptance and reliance on such forms of evidence must be tailored to the need of each case by the Judges carefully as there is no objective standard for integrity depending on the peculiarity of the system.

Position of Bangladesh

The Evidence Act, 1872 [38]. When compared with the General Clauses Act, 1897 [39]. Excludes the word ‘written’ from the definition of ‘document’. The center of attention of this statute is that the document is to be used for recording the matter. The Evidence Act further goes on that, some limited exception, when the contents of a document are to be proved, the document itself has to be adduced and copies of it shall not be admissible. The means to inspect an electronic document is by displaying it on a secondary device, either a screen or a printout. It is a justifiable argument that such display is not original, but amounts to a copy and is therefore, inadmissible as evidence. Then there must be some inclusion in the definition of document as it says that any information contained in an electronic record with is pointed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be deemed to be also a document, if the condition mentioned in this section are satisfied. Thus, with the amendment to the Evidence Law, an electronic document can for all practical purposes have the same legal effect as a paper based original document so long as the conditions mentioned in sub clauses of the amended section are satisfied. Another

route could be using the evidence for corroborative purposes. Oral evidence can be introduced if it relates to the relevant fact.

Further, under the second proviso to section 60 of the Evidence Act, if the oral evidence refers to the existence or condition of any material thing other than a document, the court may ask for the production of such material thing for inspection. Thus, if oral evidence is adduced to prove the execution of a contract, then computer evidence is admissible as it can be termed as material thing. Therefore, computer evidence is to be allowed to corroborate the oral evidence.

ICT Act, 2006 provides that, where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such information or matter is rendered or made available in an electronic form but such information or matter is accessible so as to be usable for a subsequent reference [40]. If any law provides any information or any other matter shall be authenticated by affixing the signature or any document shall be authenticated by signature or bear the signature of any person then notwithstanding anything contained in such law, such information or matter is authenticated by means of digital signature affixed in defined manner or so is the case of any document [41].

If any law provides for filing of any form, application, license, permit, payment of money or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner then notwithstanding anything contained in such law, filing, issue, grant of the document and receipt and payment of money, as the case may be, is effected by means of prescribed electronic form [42].

When any law requires that any law, rule, regulation, order, bye-law, notification or any other matter shall be in print in the Official Gazette, then, such requisite shall be deemed to have been contented if such law, rule, regulation, order, bye-law, notification or any other matter is available in the Official Gazette or Electronic Gazette but the date of publication shall be considered to be the date of the Gazette which was first published in any form [43].

However, The Evidence Act, 1872 doesn't recognize electronic evidence as a document like other printed or paper based instruments which created confusion about the application of provisions of ICT Act, 2006 relating to digital signature certificate and other electronic records. But, under the section 19(2) of The International Crimes (Tribunal) Act 1973 amended in 2009, it has been mentioned that all reports, photographs, films and other materials having evidentiary or probative value may be produced as evidence. On the other hand it is assumed that higher judiciary approves electronic records as evidence in some cases. Such as:

In '*Khaleda Akter vs State'* (37 DLR 275) case High Court held that, "The Supreme Courts in India and Pakistan approved of a tape record being used in evidence. …..During tape recording it records only sounds while a video cassette or tape records both sounds and pictures. If sound recorded on a tape is admissible as evidence, we do not make out any discrepancy in principle why the record of sound and pictures should not be similarly admissible in evidence [44].

Therefore, it is evident that the judicial decisions are acknowledging the electronic records as documents in case of production of evidence before the court though it is inconsistent to the Evidence Act, 1872.

Findings and Suggestions

In order to smooth the progress of e-commerce and promote the growth of information technology, the Information and Communication Technology (ICT) Act, 2006 was amended in 2013 enacted making provisions with a maximum punishment of 14 years imprisonment or fine up to taka 10 million or both. Unfortunately still there are definite restrictions of the said Act and also in other enactments which should be taken into consideration to make transactions more simply through electronic means. Such as:

- The Act does not touch any subject matter about various intellectual property rights like copy right, trade mark and patent right of e-information and data. Therefore, these issues must be integrated under the ICT Act, 2006 for pulling together with the separate laws on those issues.
- The legislation was hypothetically to be applied to crimes committed all over the world at the outset but nobody knows how this can be achieved in fact. This Act provides that if any foreign person commits crime under the laws of Bangladesh residing outside Bangladesh then he will be penalized but how it would be executed the Act is silent in this regard. So, international teamwork must be enhanced to work out this problem.
- Spamming has become a threat in the West as such they have made anti-spamming provisions in cyber law. However, Anti-spamming provision must be inserted in the Act.
- This law made e-mails as evidence, conflicting with the Evidence Act, 1872. It is seen that e-mail is the widespread means of communication of every transaction. So, if this electronic record is not produced before the court during any dispute then the monetary or business transaction cannot be done securely. Therefore, the provisions of the Evidence Act, 1872 must be amended in this regard.
- Police officers have been authoritative power to enter into any public place and apprehend anyone without warrant who has committed or assumed to commit crime under this Act which is often misused by police. So, definite safeguard must be inserted in this Act like issuance of warrant or prior order of the court.
- Government officials have been indemnified for their work or transaction under this Act which has been conducted in 'good faith'. But, this Act does not undoubtedly mention the extent of good faith transaction and that would give confidence the officials to be casual or reluctant to their duties which will cause severe damage of the subscriber. Therefore, certain punishment must be inserted for the negligent functioning of the officials to make sure suitable e-transaction.
- There should be an EFT (Electronic Fund Transfer) Gateway, which will unite all finance and banking institutions, ATMs, POS and related websites. Such access will accelerate the transactions among banks, commercial institutions. Introduction of this variety of infrastructure should be one of the main concerns.
- There should be a specific law and policy on e-

commerce. As regards pornography separate law has been enacted so with the elements of e-commerce which relates with internet (digital signature, internet protocol, online payment, cryptography etc.) separate law should be enacted which may play a great role in growing E-Commerce.

- The Certifying Authority and other officials (investigating officer, judges of tribunal) should be well skilled in the field of contemporary technology like internet, web-hosting etc. to accomplish their duties more productively and to ensure security to the subscriber during their transaction.

Nevertheless apart from the lacking on the ICT Act, 2006, there are huge challenges that should be overcome by our own and joint efforts with the help of government to enrich e-commerce sector.

Conclusion

The government tried to fill up gap to cyber law by passing The ICT Act, 2006. However, some issues are still not covered by the Act, which have wide ranging ramification for the growth of E-Commerce in Bangladesh. The information technology has imposed new legal problems that do not have a precedent in the common law world. The principle of common law has become inapplicable to the legal issue that has evolved in cyberspace, which knows no boundaries and physical environment. These issues do not have any solution in the existing legal regime. Thus, the legal positions pertaining to the electronic transactions as well as civil liability for the act conducted in cyberspace is still blur. The digital signature can provide a high degree of assurance that a message is originated from a particular person and that its contents could not been altered in transmission. However, no system can provide an absolute guarantee but there seems little doubt that in term of authenticating the terms of a message and the identity of the sender. A well-Managed system of encryption may be less susceptible to forgery and fraud in comparison to traditional method of contracting.

References

1. Elias M. Awad, Electronic Commerce: From Vision to Fulfillment Prentice-Hall of India Private Ltd, New Delhi, 3rd edn, 2006, 7-16.
2. ibid, pp. 51-63.
3. Supra Note 1, pp. 7-19.
4. Available at: http://www.wto.org. (Last visited on November 18, 2020).
5. Available at: http://europa.eu.int. (Last visited on November 27, 2020).
6. Islam R. "Challenges of Online Banking", *the Financial Express*, Bangladesh, 2016.
7. Andam Zorayda Ruth. E-commerce and e business, E-Asian Task Force and Asia–Pacific, 2017.
8. ibid.
9. Elias M Awad. Electronic Commerce: From Vision to Fulfillment Prentice-Hall of India Private Ltd, New Delhi, 3rd edn, 2006, 34.
10. Different web sites are: www.chorka.com, www. hutbazar.com, www.ekhanei.com, www.Mukta bazaar.com, www.bikroy.com, www.bdjobs.com, www.bestway.com etc.
11. Kaushik, Anjali. Sailing Safe in Cyberspace, SAGE Publication Ltd, London, 1st edn, 2013, 103.
12. Tabrez Ahamad. Cyberlaw E-Commerce and M-Commerce, A.P.H. Publishing Corporation, 1st edn, 2003, 88-89.
13. Chaubey RK. An Introduction to Cyber Crime and Cyber Law, Kamal Law House, Kolkata, 1st edn, 2008, 72.
14. Rahul Malthan. Law Relating to Computers and Internet, Butterworths India, New delhi, 1st edn, 2000, 132-133.
15. Kamath. Nandan. The Law Relating to Computers, Internet and E-Commerce: A Guide to Cyber Laws and the IT Act with Rules, Regulation and Notification, Universal Publication Co. 2nd edn, 2002, 146-147.
16. Supra Note 9, 455.
17. Supra Note 13, 73.
18. Supra Note 9, 454.
19. Fatima, Talat. Cybercrimes, Eastern Book Company, Lucknow, 1st edn, 2011, 112.
20. ibid.
21. ibid.
22. ibid, 113.
23. Hossein Bidgoli. Electronic Commerce: Principles and Practice, Academics, California, 2002.
24. Elias M Awad. Electronic Commerce: From Vision to Fulfillment, Prentice-Hall of India Private Ltd, New Delhi, 3rd edn, 2006, 460-463.
25. Sujeet Kumar. Encyclopaedia of Cyber Laws ABD Publishers, New Delhi, 1st edn, 2011, 187.
26. According to Section 2(33) of ICT Act, Certifying Authority is that authority who has been authorized to grant license to other in compliance with section 18 and 22 of this Act, 2006.
27. The Information and Communication Technology Act No. 39 of 2006.
28. ibid.
29. Section 38 of the Information and Communication Technology Act No. 39 of 2006.
30. Section 39 of the Information and Communication Technology Act No. 39 of 2006.
31. Dudeja VD. Cyber Crimes and Law: Cyber Crimes and Law Enforcement Commonwealth, 1st edn, 2002, 77.
32. ibid.
33. Section 42 of the Information and Communication Technology Act No. 39 of 2006.
34. Section 43 of the Information and Communication Technology Act No. 39 of 2006.
35. Development Information Programme, United Nations Development Programme. Available online at <http://www.apdip.net/publications/ iespprimers/eprimer-ecom.pdf> (last visited on December 12, 2020).
36. Article 9(1) a) of UNCITRAL Model Law on E-Commerce, 1996.
37. Supra Note 14,153.
38. Act No.1 of 1872 which came into force on September 1, 1872.
39. Act No.10 of 1897 which came into force on, 1897.
40. Section 6 of the Information and Communication Technology Act No. 39 of 2006.
41. Section 7 of the Information and Communication Technology Act No. 39 of 2006.
42. Section 8 of the Information and Communication Technology Act No. 39 of 2006.

43. Section 10 of the Information and Communication Technology Act No. 39 of 2006).
44. *Khaleda Akter vs State*, 37 DLR 275, para: 2.