Journal of Information Systems Engineering and Management
2025, 10(2)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The Security Challenges Facing Electronic Commercial Remittance Work and Ways to Confront Them

Mohamed Alkaise[1]*, Mohammed A. Sulaiman[2],
[1] *The law Department, College of Law & Political Sciences, University of Anbar, Anbar, Iraq*
Email: mohamedalkaise@uoanbar.edu.iq
[2] **Mohammed A. Sulaiman,** *The law Department, College of Law & Political Sciences, University of Anbar, Anbar, Iraq, Email: mohammed8085@uoanbar.edu.iq*

ARTICLE INFO

Received: 15 Nov 2024
Revised: 26 Dec 2024
Accepted: 16 Jan 2025

ABSTRACT

There are difficulties that affect the effectiveness of the role performed by electronic commercial remittance, and these difficulties are related to the electronic method through which it is initiated and processed. Information technology has played a significant role in the development of commercial remittance, yet at the same time, it could hinder it if proper protection and security measures are not in place. This can be attributed to the possibility of errors occurring, whether these errors are due to the individuals' entering data, technical malfunctions, or other reasons. There is also the possibility of tampering, destruction, and theft, which hinders the acceptance of electronic commercial remittance. However, there are ways to overcome the security difficulties facing electronic commercial remittance, which will be highlighted to address these challenges.

Keywords: The Security Challenges, Electronic Commercial Remittance, Ways to Confront

1. INTRODUCTION

The emergence of modern technology and continuous technological advancement has played a significant role in facilitating business transactions on a broader scale(Allioui, Mourdi, & Science, 2023; De Villiers, Kuruppu, & Dissanayake, 2021). However, at the same time, it has brought about major technological challenges, necessitating the search for effective ways to overcome the security difficulties facing electronic commercial remittance. This includes following electronic authentication procedures.(Ahuja, Prabha, Garg, & Security, 2025; Refat, 2023) If a remittance is stolen or damaged by malicious actors, one can resort to the authentication authority to obtain a copy.(Ali & Bhatti, 2024) Electronic authentication also alerts the parties to the importance of the transaction they are conducting, making them attach great importance to it, (Gupta, Dwivedi, & Shah, 2023)thereby preventing inadvertent errors such as data entry mistakes. Additionally, encryption can be employed to provide protection for the remittance against the risks of electronic attacks.

1. Importance of the Topic and Reason for Its Selection

The importance of the topic lies in the fact that electronic transfers have become a necessity in electronic banking. E-banks contribute to creating a competitive market that saves time and is indifferent to distances. However, electronic transactions also carry numerous risks that must be addressed through study and the development of suitable solutions.(Regin, Rajest, Shynu, & Finance, 2022) This is why the topic has been chosen, as it is a modern issue with few legal studies addressing the problems faced in electronic banking transfers.(Alzoubi et al., 2022; K. Jain & Chowdhary, 2021)

RESEARCH METHODOLOGY

The study relies on a comparative analytical approach, analyzing legal texts and scholarly opinions related to electronic transfers. It aims to extract solutions consistent with the unique nature of the research topic and encourages investment in the pioneering experiences of countries in regulating electronic transfers and conducting banking operations via digital technology that has been invested in this field. Consequently, the research addresses the risks of unintentional errors and ways to confront them in the first section, followed by the risks of intentional errors and their countermeasures in the second section.

1.1. Section One

Risks of Unintentional Errors and Ways to Confront Them

Unintentional errors in electronic commercial transfers may occur due to the parties' lack of knowledge in using modern electronic means, or as a result of technical malfunctions in devices or software that prevent them from performing their functions or connecting to the network. To investigate unintentional errors and how to confront them, this section will be divided into two branches: the first will discuss the risks of unintentional errors, and the second will address ways to confront them.(Chen, Kumara, & Sivakumar, 2021)

1.1.1. Branch One: Risks of Unintentional Errors

The difficulties arising from unintentional errors are involuntary risks that affect electronic documents and weaken their legal validity. This is due to the potential distortion of the data they contain during transactions, which threatens the integrity and accuracy of these documents, whether the errors originate from individuals or result from technical failures or other causes, which will be discussed in detail.(Hesami, Jenkins, & Jenkins, 2023)

A. Personal Errors:

This type of error is the most common when organizing electronic documents due to its association with the data entry process involved in these documents. Errors can also occur when sending messages over the internet, as well as in the preparation of software containing electronic chips. This may involve using inappropriate security software, improperly installing programs on a computer, or entering data into electronic chips in a manner that makes it difficult to retrieve whenever desired.(Viswanatha, Sathisha, & Kumari, 2022)

B. Technical Errors:

A technical error occurs due to malfunctions of the hardware and software used in extracting electronic documents. These errors are viewed from a technical perspective and include issues affecting devices and the data stored in them, often due to cyberattacks or viruses. Examples include:

1) Malfunctions affecting computers and operating or communication software due to viruses or hacker attacks.(Belous & Saladukha, 2020)
2) Problems preventing internet connectivity, which may occur due to personal device malfunctions that deny access to internet services, or issues with the service provider’s equipment caused by viruses, natural conditions, or other reasons.(Dridi, Radhakrishnan, Moser-Mercer, DeBoer, & Learning, 2020)
3) Malfunctions in computer programs that mislead the sender into believing that a transmission has occurred when it has not actually been sent or received by the intended recipient.(MacFarlane, Missaoui, Makri, & Gutierrez Lopez, 2022)

Technical errors differ from personal errors in that the former occur in the electronic devices and software used to generate the documents, while the latter are committed by the individual responsible for entering the data and information within the electronic documents. Technical errors are less frequent compared to personal errors, which are more common due to their link to the data entry process that relies on manual input. However, the recurrence of technical errors poses challenges for electronic documents and affects individuals' willingness to engage with them. Overcoming technical error difficulties depends on the development and efficiency of the electronic technologies that can be relied upon for handling electronic commercial transactions.

C. *Errors Due to External Circumstances*

These errors arise from the surrounding environmental conditions and their impact on the computers that generate electronic documents, particularly in the processes of organizing and transferring information and validating legal actions. Such external factors include adverse weather conditions, fluctuations in temperature and humidity, the presence of dust or sand, and natural disasters like fires and floods, which can disrupt internet services. Additionally, power outages affecting electronic devices can lead to malfunctions and errors that jeopardize the integrity of the data contained in the documents, both in terms of their storage and transmission.(Liu et al., 2022; Zangana, 2022)

Despite the advancements in modern communication technologies, these risks remain possible and have become more serious than before, due to the vast number of transactions processed by each device in a short time when generating electronic documents. The increased volume of electronic transactions raises the likelihood of errors.

Unlike Iraqi and Egyptian legislators, who have not addressed the issue of unintentional errors, American legislation has tackled this problem. It grants parties to any electronic transaction the right to agree on security measures to detect errors or changes in the electronic document, thus avoiding the effects of such errors or changes.

If the electronic transaction occurs through an electronic agent and an error or change results, the recipient must follow specific procedures, including notifying the sender of the error and informing them that they will not be bound by the received electronic document. They must follow the instructions of the other party regarding the return or deletion of the erroneous electronic document and must not use or benefit from it; otherwise, the change or error will remain in effect.

This is addressed in Article 9 of the Uniform Electronic Transactions Act (UETA), which states:(Warren & Lawless, 2024)

(A) If a change or error occurs in the electronic record during its transmission between the parties to the transaction, the following must be observed:

1) If the parties have agreed to implement a security procedure to detect changes or errors, and one party has acted according to that procedure while the other has not, if the non-compliant party discovers the change or error and subsequently agrees to that procedure, they may void the effect of the change or error.
2) If a person conducts an electronic transaction, they may avoid the consequences of the electronic error by dealing with another person's electronic agent. If the electronic agent does not provide an opportunity to prevent or correct the error, that person must:

a) Immediately notify the other person of the error and inform them that they did not intend to be bound by the received electronic record.
b) Take appropriate steps, including agreeing to the acceptable instructions set by the other person, and return or delete what they received from the other party through the erroneous electronic record.
c) Not use or benefit from what they received from the other party.

(B) If paragraphs 1 and 2 of this article do not apply, the change or error will remain in effect.

(C) Parties may not agree to deviate from the provisions of paragraph 2 of (A) and paragraph (B).

1.1.2. Branch Two: Ways to Address the Risks of Unintentional Errors

The risks of unintentional errors can be mitigated by resorting to electronic documentation for the electronic transfer, as following documentation procedures alerts the parties to the importance of the actions they undertake, leading them to give it significant attention. Additionally, the involvement of a third party (the notary) can warn the parties of any mistakes they may make. Therefore, electronic documentation enhances the guarantees of electronic commercial transfers and helps to overcome their difficulties. The entity responsible for electronic documentation may be either private or public, where the private entity refers to electronic certification bodies mentioned in electronic transaction laws, while the electronic notary represents the public entity for documentation.(Yarovenko, Bilan, Lyeonov, Mentel, & management, 2021)

The importance and necessity of electronic documentation have increased due to developments in the framework of electronic commercial transactions. (V. Jain, Malviya, Arya, & government, 2021)It allows participants to electronically verify the identity of those they deal with or their capacity to commit under the transfer, helping to overcome many of the challenges faced. The procedures for electronic documentation and the entities responsible for it will be addressed in the following points:

1.1.2.1. Electronic Certification

Electronic certification has a significant impact on the validity and authenticity of electronic documents, which supports trust in them and guarantees the rights of parties dealing through electronic means. It assures them that the electronic writing has not been altered. Electronic certification provides confidence and security in electronic commercial transfers, ensuring they have not been modified or tampered with. It also allows for verification that the signature belongs to the drawer, thus helping to overcome difficulties in their transactions, especially security-related challenges.(Maulani et al., 2021; Rahardja, Hidayanto, Putra, Hardini, & technology, 2021) The provisions of electronic certification will be discussed in the following points:

a) Definition of Electronic Certification

Electronic certification is defined as a set of procedures aimed at achieving trust and security by linking the electronic signature to the signer with certainty and ensuring it originates from someone authorized to perform the legal act mentioned in the electronic document. It is also defined as a technical process aimed at verifying that the public key of the electronic signature is linked to the private key belonging to the signer. No definition of electronic certification exists in Iraqi law, nor in Egyptian law. The American legislator, on the other hand, did not refer to electronic certification in the specific provisions of electronic legislations but permitted electronic documents to be certified by a notary, as will be seen later. Regarding electronic commercial transfers, it can be defined as the intervention of a neutral third party for certification, ensuring that the signature on it is guaranteed and authenticated, thus preventing any possibility of manipulation or alteration in its content.

b) Nature of Electronic Certification

Electronic certification is considered, in terms of its nature, one of the required conditions for recognizing the validity of electronic signatures. This is consistent with the Iraqi legislator's stance in Article 5 of the Electronic Signature and Electronic Transactions Law, which states that electronic signatures may be valid for proof if they are certified by a certification body. Therefore, if the condition of certification by the relevant authority is not met, the electronic signature will lack legal validity. The Egyptian legislator did not refer to such a role for electronic certification.(Capece, Levialdi Ghiron, & Pasquale, 2020)

c) The Entity Responsible for Electronic Certification

The entity that undertakes certification procedures is referred to as the "certification body," defined as the entity that provides electronic certificates to the public or offers them services related to electronic signatures. The Iraqi legislator defined it in the fifteenth clause of Article 1 of the Electronic Signature and Electronic Transactions Law as "the certification entity, a legal person authorized to issue electronic signature certification according to the provisions of this law." The licensing authority is the General Company for International Information Network Services, after obtaining the approval of the Minister of Communications. Article 1 of the same law states that the company is responsible for: first, granting licenses to issue certification certificates after obtaining the minister's approval in accordance with the law. Article 7 of the same law prohibits practicing electronic certification activities without obtaining a license from the relevant authority, stating that "no one shall engage in the activity of issuing certification without obtaining a license according to the provisions of this law." As for the Egyptian legislator, it did not define the certifying body but transferred the responsibility to the Information Technology Industry Development Authority, which grants the necessary licenses for electronic certification bodies. Article 4 of the Electronic Signature Law states that "the authority shall carry out the necessary functions to achieve its objectives, particularly the following: (a, issuing and renewing the necessary licenses to engage in electronic signature services and other activities in the field of electronic transactions and information technology, in accordance with the provisions of the laws and regulations governing them)." Article 19 of the same law prohibits the practice of issuing certification certificates without the approval of the Information Technology Industry Development Authority, stating that "the activity of issuing electronic certification certificates may only be practiced with a license from the authority, for a fee determined by its board of directors according to the procedures, rules, and guarantees set forth in the executive regulation of this law."

d) Liability of Certification Authorities:

The liability of a certification authority arises from its failure to fulfill its obligations, which will vary depending on whether its obligation is to achieve a result or to exercise care. If the obligation is to achieve a specific result, the authority is liable upon failure to do so, and it bears the burden of proving an external cause if it seeks to avoid liability; here, negligence is presumed. Conversely, if the obligation is merely to exercise care, fulfilling its duties requires only a reasonable level of care and the adoption of all possible measures to perform its functions effectively. This is because the obligation of electronic certification authorities is akin to service contracts, where the only requirement is to exercise necessary care. Therefore, the mere failure to issue a certificate does not constitute an error warranting liability; rather, the burden of proof lies with those claiming negligence against the electronic certification authorities. This interpretation could undermine the guarantees ensuring the proper functioning of electronic certification authorities, as it shifts the burden of proof to the harmed party. Thus, we view the obligation of certification authorities as one to achieve a result, as evidenced by the legal texts above, which outline their obligations in a direct manner (i.e., "the licensed authorities must provide the company or relevant court with what is requested...").

There must be a role for public authority in the operations of electronic certification authorities, considering their purpose in certifying documents, ensuring their confidentiality, and securing the information they contain. Indeed, the Iraqi legislator has granted the General Company for International Information Network Services the right to oversee electronic certification authorities, address complaints against them, provide advice, and conduct training sessions to ensure proper performance. This is outlined in Article 1 of the Electronic Signature and Electronic Transactions Law, which states that the company is responsible for: 1) monitoring and supervising the performance of entities issuing certification; 2) addressing complaints regarding electronic signature activities; 3) providing technical advice to those working in electronic signature and certification; and 4) conducting training sessions and educational conferences in this regard. Similarly, the Egyptian legislator has granted the Information Technology Industry Development Authority the right to suspend or revoke the license of electronic certification authorities if they violate licensing conditions or legal provisions, as stated in Article 26 of the Electronic Signature Law.

1.1.2.2.The Electronic Notary

A notary public is generally an official with the necessary legal qualifications, responsible for documenting legal acts, except for those specifically excluded, in order to confer official status and protect the documented legal acts, including commercial transactions and commercial papers. The following conditions must be met for a notary public: 1) a bachelor's degree in law, and 2) completion of a judicial institute course of no less than three months.

An electronic notary is a neutral person entrusted by parties to certify their documents, verifying their validity and the circumstances surrounding them. Acting as a third party, the electronic notary provides electronic certification to confirm the authenticity of electronic transactions via an electronic record containing relevant information, keeping a copy of the documents certified.

Article 1 of the Iraqi Notary Law No. 33 of 1998 states that the law aims to: 1) organize and document legal transactions, affirming the rights arising from them and conferring official status; and 2) ensure protection for the legal acts documented by the notary, verifying the identities of the parties involved. This protects electronic commercial transfers from loss due to electronic theft or damage, as the holder can obtain a copy from the notary's stored records. If a transfer is altered, the original text can be verified by referring to the electronic notary's records.

The electronic notary must use reliable methods to certify transfers to gain the trust of individuals interacting with them, taking reasonable steps to ensure the accuracy and integrity of the certified transaction. They should also provide accessible means for parties to verify these methods by consulting the electronic notary office that documented the transfer.

It should be noted that the Iraqi Electronic Signature and Electronic Transactions Law does not specify the existence of electronic notaries, implying that the role may be performed electronically. However, this requires legal organization, necessitating amendments to the Electronic Signature Law or the Notary Law to outline the necessary procedures for electronic notary offices.

1.2.Section Two:

The Risks of Intentional Errors and Ways to Address Them

Some individuals may commit errors with the intention of causing harm to the parties involved in a transaction. Such errors can result in civil liability for the perpetrator, or even criminal liability if the error constitutes a violation of criminal law, such as when the act involves theft, damage, or forgery of the transaction. In this section, we will explore the risks of intentional errors and the means to confront them, which we divide into two parts: the first addresses the risks of intentional errors, and the second focuses on ways to address them.(Srinivasan & Sarial-Abi, 2021)

1.2.1. Risks of Intentional Errors

1.2.1.1. Intentional Electronic Error:

This refers to unlawful behavior, whether it results in civil or criminal liability. An intentional electronic error causing civil liability involves any breach of a contractual or legal obligation coupled with awareness, such as when internet service providers fail to fulfill their contractual obligation to provide the agreed service, causing harm to their clients, which leads to the company's civil liability.

On the other hand, an intentional electronic error causing criminal liability involves any behavior that violates penal laws, resulting in an electronic crime. This type of crime is defined as an illegal activity aimed at copying, altering, deleting, or accessing stored information within a computer or transmitted via it. It can also be defined as any action that violates the law and is committed using computers and the internet.

In the context of our study of electronic crimes related to electronic commercial transactions, we favor the first definition because it focuses on acts related to tampering with the content of a document and accessing it unlawfully, which is relevant to electronic commercial transactions, as these are considered both a document and property. The second definition is broader and does not limit itself to electronic crimes involving documents and electronic assets but extends to other forms of electronic crimes, such as moral crimes.

Some argue that unlawful acts committed using computers and the internet should not be deemed crimes due to the principle that there is no crime or punishment without a legal text and that analogies cannot be used to create new crimes. As no law has yet been enacted to criminalize such acts, they cannot be considered crimes. Thus, the resulting liability can only be civil. However, some believe these acts should be considered crimes without the need for specific legislation because existing traditional laws apply, not by analogy but because these crimes align conceptually with those listed in penal codes, such as theft, damage, and fraud, differing only in method and means. Criminal law does not emphasize the means by which a crime is committed. We support this view to prevent offenders from escaping accountability due to the absence of specific cybercrime laws. However, this does not negate the need for legislation regulating cybercrimes and prescribing appropriate penalties.(Kaplan, Weisberg, & Binder, 2021)

In our study of electronic crimes, we will limit our focus to the criminal behavior constituting the material element of the crime, given its distinct nature within the framework of electronic commercial transactions.(Qin, Wang, & Hui, 2022) We will not delve into other aspects to avoid overburdening the research with details specific to criminal law. The electronic crimes under discussion are those involving property, considering that electronic commercial transactions are movable assets susceptible to crimes typically committed against property, such as:

1.2.1.2.The Crime of Information Theft:

This crime occurs when information systems are breached by unauthorized individuals, commonly known as hackers. The intent behind this unauthorized access is to seize and take possession of the stored data, including electronic commercial transactions.

The tools used for system breaches include software readily available on the internet, which skilled individuals can use to launch attacks on others' devices. Typically, such breaches target computers connected to the internet, linking victims' devices with those of hackers. Consequently, hackers can access data from electronic commercial transactions, including personal banking information, which enables them to steal from the accounts of the involved parties.

The Arab Convention on Combating Information Technology Crimes addresses this in what it considers a crime of unauthorized access. Article (6) states:

1. Unauthorized access, presence, or any unauthorized connection with all or part of an information system, or continuation thereof.
2. Penalties are increased if the unauthorized access, presence, or connection results in:

a. Deletion, modification, distortion, copying, transfer, or destruction of stored data, electronic devices, systems, or communication networks, and causing harm to users and beneficiaries.

b. Obtaining confidential government information, where the terms "copying or transferring" in the above text refer to theft.

1.2.2. The Crime of Illegal Interception:

This crime, referenced in Article (7) of the Arab Convention on Combating Information Technology Crimes, involves the deliberate and unjustified interception of data transmissions by technical means, disrupting or stopping the transmission or reception of data. This crime is closely related to electronic theft since the offender's primary goal is usually to seize the intercepted data.

1.2.3. The Crime of Electronic Forgery:

Electronic forgery involves altering the truth in an electronic document, posing a more severe threat than traditional forgery. Its danger lies in its reliance on technical foundations, making it difficult to detect, unlike forgery in paper documents. If a system is breached, the hacker can alter the content of an electronic commercial transaction, a process referred to in financial law as "falsification." The Arab Convention on Combating Information Technology Crimes addresses electronic forgery in Article (10), which states: “Using information technology means to alter the truth in data in a way that causes harm, with the intent of using it as accurate data.”

1.2.4. Crimes of Electronic Asset Destruction:

These crimes aim to damage another's property, either by total or partial destruction or by preventing access to it, rendering it unusable for its intended purpose. Electronic destruction crimes are technical behaviors that involve using specific viruses capable of destroying electronic systems and all stored data. The most common types include:

- **Chernobyl Virus**: A virus that activates on a specific date, May 21st each year, causing damage only on that day.
- **Worm Virus**: A rapidly replicating virus that copies itself on a computer and spreads to others via infected emails or disks.
- **Trojan Horse Virus**: A highly dangerous virus that spreads through various communication methods. It not only destroys programs and data but also spies on individuals and companies, sending secret information to hackers and specialists.
- **Time Bomb Virus**: A virus that remains dormant until a specific event, date, time, or user action trigger it, leading to the destruction of stored programs and data, which can disrupt computer programming.

The Arab Convention on Combating Information Technology Crimes addresses the crime of destruction under the term “Assault on Data Integrity” in Article (8), which states:

1. Intentional and unjustified destruction, deletion, obstruction, modification, or concealment of information technology data.
2. A party may criminalize the acts specified in paragraph (1) of this article if they cause severe damage.

1.2.5. The Crime of Unlawful Use of Electronic Payment Tools:

This crime is mentioned in Article (18) of the Arab Convention on Combating Information Technology Crimes, which states:

1. Anyone who forges, fabricates, or sets up any devices or materials to assist in forging or counterfeiting any electronic payment tool by any means.
2. Anyone who seizes the data of any payment tool and uses, transfers, or facilitates others’ access to it.
3. Anyone who unlawfully uses the internet or any information technology means to access the numbers or data of any payment tool.
4. Anyone who knowingly accepts a counterfeit payment tool.

Since electronic commercial transactions are a form of electronic payment, the provisions of this crime apply to them.

General Characteristics of Cybercrime:

Cybercrimes are generally challenging to prove as they are committed using computers and the internet by highly skilled individuals in information technology, enabling them to conceal their actions and erase traces, making it difficult to track the perpetrator. Additionally, victims often hesitate to report such crimes to authorities due to ignorance of the offender, fear of revealing secrets, or concern about losing clients' trust, especially if the victim is a financial institution.

1.3. Section Two:

Measures to Address the Risks of Intentional Errors**

Intentional errors can be mitigated by implementing electronic documentation procedures. Utilizing a certification authority allows one to obtain a copy of a document in cases of theft, destruction, or forgery of its content. Documentation procedures have been previously discussed, so we refer back to them to avoid repetition. Another way to mitigate these risks is through the use of encryption, a system that is not new but has been used historically in intelligence, military, political, and diplomatic fields. With the growth and spread of electronic technologies and the internet, encrypted writing has become an essential tool for ensuring the security, confidentiality, and integrity of electronic commercial transactions. Encryption has emerged as a crucial measure to secure electronic transactions by encoding them into an unreadable format that is inaccessible to intruders, thereby preventing theft or manipulation of the content.

Electronic commercial transactions, which are among the most important electronic payment methods, must be protected to perform their functions optimally. One of the most effective protection measures is encryption, which will be discussed in the following points:

1.3.1. Definition of the Encryption System

Encryption is defined as the science of creating a system for coded writing. Coded writing systems are methods for transmitting messages in a specific way by converting them into symbols and signals that cannot be accessed or altered by unauthorized persons. These messages are only accessible to specific individuals who can translate and read them using specific keys; without these keys, the messages cannot be read. Encryption is a procedure used to verify that a document or electronic signature has not been altered or corrupted by using algorithms or other codes. It is also defined as a technique based on a smart mathematical algorithm that allows someone with a secret key to convert a readable message into an unreadable one and vice versa, using the secret key to decrypt and revert the encrypted message to its original state. For an encryption system to be reliable, the algorithm used must be highly effective, designed so that decrypting the message without the secret key is nearly impossible. Encryption essentially converts comprehensible information into incomprehensible data, which can be reverted to its original state using the secret key or another corresponding key.(Kaur & Kumar, 2020)

Neither Iraqi nor Egyptian lawmakers have explicitly regulated encryption by permitting or prohibiting it, which can be interpreted as an allowance to use encryption systems to protect electronic documents. In contrast, U.S. legislation has adopted encryption, calling it a "security procedure." According to Section 1-201 of the Uniform Electronic Transactions Act (UETA), it is defined as: "(A security procedure) means a procedure employed to verify that an electronic signature, record, or performance was that of a specific person or to detect changes or errors in the information contained in the electronic record. (A security procedure) includes any process that requires using algorithms, codes, identifying words and numbers, reversal procedures, or any other similar methods." This definition highlights that encryption ensures that the electronic document and signature originate from the intended person and are free from alterations or changes. It also emphasizes the means used in encryption, such as mathematical algorithms, symbols, and numbers.(Emmert, 2022)

The encryption process consists of three stages:

1. Writing the information that needs to be changed while maintaining its confidentiality.
2. Using a secret key to convert readable information into unreadable data.
3. Using the same key employed in encryption or a different key to decrypt and revert the information to its readable state. Thus, encryption occurs before sending the message and is decrypted after reaching the recipient.

1.3.2. Types of Encryption

Encryption can be classified based on how legislators regulate it into two types:

1. **Broad Concept of Encryption**: This type refers to the use of encryption tools without any restrictions.
2. **Narrow Concept of Encryption**: This involves implementing strict measures and monitoring the use of encryption tools by the state. Although this restricted form of encryption allows the state to oversee electronic commercial activities, it has limitations, making it easier for hackers to break the encryption. On the other hand, the broader concept of encryption is unrestricted, making it difficult to penetrate. However, its drawback is that it can impede the application of state regulations, such as taxation and monitoring of transactions and commercial activities, thus providing opportunities for legal evasion. Nevertheless, the benefits of protecting electronic transactions outweigh its drawbacks.

It appears that comparative laws, including Iraqi, Egyptian, and American legislation, have adopted the broader concept of encryption, as they do not specify restrictions on the encryption process. This implies that they have left the door open for the use of any feasible technology to encrypt electronic documents without being bound by specific encryption limits.

From a technical perspective, encryption is divided into several types, which are explained in the following points:

1. **Symmetric Encryption:**

This type of encryption uses the same key or secret code for both encrypting and decrypting the document. In other words, symmetric encryption systems work using a single key, known as the private key, which is shared by both the sender and the receiver of the message.
The drawback of this type of encryption is that the receiver, who gets documents from various sources, must have a number of keys equal to the number of incoming documents from those sources. Another issue is the possibility of the encryption key being exposed, as the same key is used by two different people. This poses a risk because the key could be unlawfully transferred to others, and it would be challenging to detect such transfers, especially since both the sender and receiver possess the same key.(Zhang, 2021)

2. **Asymmetric Encryption:**

Unlike symmetric encryption, asymmetric encryption does not use the same key or code for encrypting and decrypting the document. Instead, it employs two different keys: one private key known only to a specific user and kept secret, and one public key distributed or communicated to other users who wish to send encrypted messages.
Based on this setup, anyone with the public key can use it to encrypt messages and send them to the user holding the private key. Conversely, only the user with the private key can decrypt the incoming documents and read them. This encryption method provides a high level of confidentiality; however, it is not without risks. Hackers, especially highly skilled ones, may try to infiltrate the network during the public-private key verification process by using precise mathematical algorithms. Therefore, it is advised to keep the verification period short, making it difficult for hackers to exploit it. It is also recommended to change the encryption keys periodically and increase the number of digits in the keys to complicate decryption.(Zhang, 2021)

3. **Encryption Using Electronic Document Security Techniques:**

This type of encryption utilizes both the public and private keys for encrypting and decrypting the document. It provides confidentiality and security for electronic documents, ensuring that only the sender and receiver can access the content. To illustrate how this works, consider two people (A and B), each with their own private keys, who want to securely communicate. Party A encrypts the message using their private key, then re-encrypts it using Party B's public key. Upon receiving the message, Party B decrypts it with their private key and then again with Party A's public key. This method makes it impossible for an intruder to decrypt the message unless they have both the public and private keys of both parties. This type of encryption essentially repeats the asymmetric encryption process in reverse order.(Seth et al., 2022)

4. **Encryption Using Digital Signatures:**

A digital signature is a numerical fingerprint generated according to a specific algorithm known as a hashing function. These algorithms apply mathematical calculations to the message, creating a fingerprint that represents the document. This fingerprint, typically ranging between 128 and 160 bits, uniquely identifies the original document, such that any alteration—even by a single bit—will result in a completely different fingerprint. It is impossible to generate the same digital fingerprint from two different messages. Digital signatures are created using specific private keys and can only be decrypted using their corresponding public keys, making it a unidirectional hashing function. Notably, using a digital signature algorithm is faster than asymmetric encryption, which is why it often replaces it.

5. **Encryption Using Message Concealment Techniques:**

Concealment techniques hide the document within another message, making it appear as an ordinary message. If intercepted, the hidden document is not easily detected. There are various programs, some available for free online, that can hide a text message inside a digital image. When viewed, this image looks normal, and even if the hidden message is discovered, it will still be encrypted and unreadable. However, it is worth noting that free online programs often have poor quality, making it easier to detect the hidden text, so it is advisable to use high-quality software. This method is particularly suitable for hiding electronic commercial documents during digital transfers, preventing hackers from discovering and stealing them.

If the above types of encryptions protect electronic commercial documents during online transactions, a question arises about how to safeguard these documents while still stored on the personal computers of the parties involved. One solution is the use of a "firewall," one of the most essential tools for preventing unauthorized access to information stored on a computer connected to the internet. Firewalls protect the computer or the communication channel it uses from eavesdropping by blocking unauthorized persons from accessing information related to electronic commercial documents.

1.3.3. Evaluating the Role of Encryption Systems in Protecting Electronic Commercial Documents (Atadoga et al., 2024)

Encryption systems protect electronic commercial documents by ensuring confidentiality, preventing unauthorized parties from viewing their content during internet transfers. They provide this protection through encryption systems' capabilities, which make decrypting the encoded documents extremely difficult. These systems generate new keys with each encryption process, so even if a key used in one operation is discovered, it does not enable decrypting other documents. To ensure the encryption system is reliable, the encryption tools must keep pace with rapid advancements in information technology, as encryption software may have vulnerabilities that can be exploited. Therefore, staying updated with technological developments is essential to detect and address any potential breaches.

Thanks to the security encryption technologies provide for electronic commercial documents during transmission and reception, there is no reason to believe these electronic documents are less secure than their paper counterparts. These technologies help avoid the following risks:

1. Accessing Data of the Electronic Commercial Document and Other Confidential Information Such as Personal Banking Data.
2. Attempting to Modify the Content of the Document.
3. Resending It to Another Destination.
4. Impersonating One of the Parties Involved in the Document.

However, the question arises about the level of protection that an encryption system can provide for electronic commercial documents. In reality, despite the claims about the effectiveness of encryption in protecting electronic commercial documents, experts in information security argue that such protection cannot reach perfection, i.e., achieving 100% security, for the following reasons:

1. **Electronic Protection Programs Are Not Sufficient**:
There are no protection tools capable of countering all attacks launched by intruders, even in technologically advanced countries, because electronic threats grow proportionally with the development of protection methods.

2. **Some Protection Systems Are Highly Expensive**:
High costs make it difficult for users to acquire them, leading them to opt for less expensive, less efficient programs that expose users to greater electronic risks.(Krasner, 2021)

3. **Lack of Respect for Intellectual Property Rights:**
Protection programs and encryption systems are the creations of specific individuals whose inventions must be safeguarded, allowing them to exclusively benefit financially from their innovations. The digital environment, however, does not provide such protection, with unauthorized copying and distribution of these innovations, discouraging inventors from developing or creating new protection systems due to the lack of exclusive benefits.(Mehanoor, Ahmed, & Learning, 2024)

In light of the above, it becomes clear that encryption systems cannot provide complete protection for electronic commercial documents. This has led some to advocate for an effective legal means to protect electronic transactions from cyber threats: cyber risk insurance. This involves the party using electronic means (the insured) transferring the burden of electronic risks (the insured risk) to an insurance company (the insurer) according to the terms of the insurance contract.

It is worth noting that insurance typically covers risks involving money and property, and there is no doubt that an electronic commercial document constitutes valuable property that can be insured against the risks that threaten it, especially since comparative laws have recognized the legal validity of electronic documents equivalent to their paper counterparts. As previously discussed, we refer to this point to avoid repetition. Moreover, there are U.S. judicial applications confirming this; for instance, the Minnesota Court of Appeals ruled in 1991 that electronic data stored on a computer constitutes tangible property.(Grimmelmann & Mulligan, 2022)

Conclusion

From our study of this subject, we reached several conclusions, followed by a set of proposals as follows:

Findings:

1. There Are Challenges Facing Electronic Commercial Documents:
These include intentional and unintentional errors, such as cybercrimes, which are risks believed to be inadequately addressed by current legal measures.

2. Electronic Authentication Methods Are Crucial Legal Tools:
These include electronic certification authorities and electronic notaries, which help electronic commercial documents overcome the difficulties they face, noting that some legal systems do not explicitly refer to electronic notaries.

3. Electronic Encryption Systems Are Among the Most Important Technical Tools:
These systems can be used to protect electronic commercial documents effectively.

Recommendations:

1. Call on Judicial Authorities to Address Cybercrimes According to Existing Penal Laws:
Until a specific cybercrime law is enacted, cybercrimes should be treated according to existing criminal laws, as cybercrimes differ from traditional crimes only in the method of execution. Criminal law does not consider the means by which a crime is committed, so cybercrimes cannot be considered lawful actions based on the principle "no crime, no punishment without law."

2. Explicitly Refer to the Use of Encryption in Protecting Electronic Transactions:
We suggest limiting the use of extensive encryption methods to allow relevant state authorities to monitor online commercial activities. As seen, the use of broad encryption prevents authorities from monitoring commercial activities, hindering their functions, such as tax imposition. We propose the following wording: "It is permissible to use uncommon codes or symbols that render the electronic information intended to be transmitted or sent incomprehensible to others. Codes or symbols that

make the information inaccessible without them may also be used, provided that this does not impede the competent state authorities from performing their duties."

3. Urge Insurance Companies to Consider Cyber Risks as Covered Risks:
This would make insurance policies a means to mitigate damages caused by cyber risks. We also recommend regulating the provisions of cyber risk insurance, similar to other covered risks, such as fire insurance and life insurance.

Conflict of interest: There is no conflict of interest

REFERENCES

[1] Ahuja, B., Prabha, C., Garg, G. J. S. I. o. A., & Security, M. f. E.-C. D. (2025). Emerging Technologies in E-Commerce Security. 235-260.

[2] Ali, A., & Bhatti, B. M. (2024). *Spies in the Bits and Bytes: The Art of Cyber Threat Intelligence*: CRC Press.

[3] Allioui, H., Mourdi, Y. J. I. J. o. C. E., & Science, D. (2023). Unleashing the potential of AI: Investigating cutting-edge technologies that are transforming businesses. *3*(2), 1-12.

[4] Alzoubi, H. M., Ghazal, T. M., Hasan, M. K., Alketbi, A., Kamran, R., Al-Dmour, N. A., & Islam, S. (2022). *Cyber security threats on digital banking*. Paper presented at the 2022 1st International Conference on AI in Cybersecurity (ICAIC).

[5] Atadoga, A., Farayola, O. A., Ayinla, B. S., Amoo, O. O., Abrahams, T. O., Osasona, F. J. C. S., & Journal, I. R. (2024). A comparative review of data encryption methods in the USA and Europe. *5*(2), 447-460.

[6] Belous, A., & Saladukha, V. (2020). *Viruses, Hardware and Software Trojans: Attacks and Countermeasures*: Springer Nature.

[7] Capece, G., Levialdi Ghiron, N., & Pasquale, F. J. S. (2020). Blockchain technology: Redefining trust for digital certificates. *12*(21), 8952.

[8] Chen, Y., Kumara, E. K., & Sivakumar, V. J. A. o. O. R. (2021). Invesitigation of finance industry on risk awareness model and digital economic growth. 1-22.

[9] De Villiers, C., Kuruppu, S., & Dissanayake, D. J. J. o. b. r. (2021). A (new) role for business–Promoting the United Nations' Sustainable Development Goals through the internet-of-things and blockchain technology. *131*, 598-609.

[10] Dridi, M. A., Radhakrishnan, D., Moser-Mercer, B., DeBoer, J. J. T. I. R. o. R. i. O., & Learning, D. (2020). Challenges of blended learning in refugee camps: When internet connectivity fails, human connection succeeds. *21*(3), 250-263.

[11] Emmert, F. J. T. A. J. o. C. L. (2022). Cryptocurrencies: The impossible domestic law regime? , *70*(Supplement_1), i185-i219.

[12] Grimmelmann, J., & Mulligan, C. J. A. U. R. (2022). Data Property. *72*, 829.

[13] Gupta, A., Dwivedi, D. N., & Shah, J. (2023). Overview of technology solutions. In *Artificial Intelligence Applications in Banking and Financial Services: Anti Money Laundering and Compliance* (pp. 25-39): Springer.

[14] Hesami, S., Jenkins, H. P., & Jenkins, G. P. J. A. a. S. (2023). Emerging Digital Technologies to Improve Tax Compliance and Administration Efficiency: A Systematic Literature Review.

[15] Jain, K., & Chowdhary, R. J. A. P. J. o. I. S. (2021). A Study on Intention to Adopt Digital Payment Systems in India: Impact of COVID-19 Pandemic. *31*(1), 76-101.

[16] Jain, V., Malviya, B., Arya, S. J. T. j. o. c. i. i. b., & government. (2021). An overview of electronic commerce (e-Commerce). *27*(3), 665-670.

[17] Kaplan, J., Weisberg, R., & Binder, G. (2021). *Criminal law: Cases and materials*: Aspen Publishing.

[18] Kaur, M., & Kumar, V. J. A. o. C. M. i. E. (2020). A comprehensive review on image encryption techniques. *27*(1), 15-43.

[19] Krasner, H. J. P. C. I. S. Q. (2021). The cost of poor software quality in the US: A 2020 report. *2*.

[20] Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. J. F. i. p. (2022). Cyber security threats: A never-ending challenge for e-commerce. *13*, 927398.

[21] MacFarlane, A., Missaoui, S., Makri, S., & Gutierrez Lopez, M. J. J. o. D. (2022). Sender vs. recipient-orientated information systems revisited. *78*(2), 485-509.

[22] Maulani, G., Gunawan, G., Leli, L., Nabila, E. A., Sari, W. Y. J. I. J. o. C., & Management, I. S. (2021). Digital certificate authority with blockchain cybersecurity in education. *1*(1), 136-150.

[23] Mehanoor, S. H., Ahmed, S. J. T. G.-B. H. w. A., & Learning, M. (2024). 10 Safeguarding Data and Ensuring Security in Digital Healthcare. 160.

[24] Qin, H. X., Wang, Y., & Hui, P. J. a. p. a. (2022). Identity, crimes, and law enforcement in the metaverse.

[25] Rahardja, U., Hidayanto, A. N., Putra, P. O. H., Hardini, M. J. J. o. a. r., & technology. (2021). Immutable ubiquitous digital certificate authentication using blockchain protocol. *19*(4), 308-321.

[26] Refat, M. M. H. (2023). Adoption of Digital Payment Systems in Microcredit Operations: Challenges & Opportunities in the Context of Bangladesh.

[27] Regin, R., Rajest, S. S., Shynu, T. J. C. A. J. o. I. o. T. M., & Finance. (2022). Impact of internet banking on the efficiency of traditional banks. *3*(11), 85-102.

[28] Seth, B., Dalal, S., Jaglan, V., Le, D. N., Mohan, S., & Srivastava, G. J. T. o. E. T. T. (2022). Integrating encryption techniques for secure data storage in the cloud. *33*(4), e4108.

[29] Srinivasan, R., & Sarial-Abi, G. J. J. o. M. (2021). When algorithms fail: Consumers' responses to brand harm crises caused by algorithm errors. *85*(5), 74-91.

[30] Viswanatha, V., Sathisha, B., & Kumari, A. (2022). *Custom hardware and software integration: bluetooth based wireless thermal printer for restaurant and hospital management.* Paper presented at the 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon).

[31] Warren, E., & Lawless, R. M. (2024). *Bankruptcy and Article 9: 2024 Statutory Supplement*: Aspen Publishing.

[32] Yarovenko, H., Bilan, Y., Lyeonov, S., Mentel, G. J. J. o. b. e., & management. (2021). Methodology for assessing the risk associated with information and knowledge loss management. *22*(2), 369-387.

[33] Zangana, H. M. J. A. J. o. N. U. (2022). Improving The Web Services for Remittance Company: Express Remit as a Case Study. *11*(3).

[34] Zhang, Q. (2021). *An overview and analysis of hybrid encryption: the combination of symmetric encryption and asymmetric encryption.* Paper presented at the 2021 2nd international conference on computing and data science (CDS).