Investigation of Cyber-Security and Cyber-Crimes in Oil and Gas Sectors Using the Innovative Structures of Complex Intuitionistic Fuzzy Relations

Naeem Jan [1], **Abdul Nasir** [1], **Mohsin S. Alhilal** [2,*], **Sami Ullah Khan** [1], **Dragan Pamucar** [3] and **Abdulrahman Alothaim** [2,*]

[1] Department of Mathematics, Institute of Numerical Sciences, Gomal University, Dera Ismail Khan 29050, Pakistan; naeem.jan.7300@gmail.com (N.J.); theabdulnasir@gmail.com (A.N.); gomal85@gmail.com (S.U.K.)

[2] STC's Artificial Intelligence Chair, Department of Information Systems, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia

[3] Department of Logistics, Military Academy, University of Defence in Belgrade, 11 000 Belgrade, Serbia; dragan.pamucar@va.mod.gov.rs

* Correspondence: moalhilal@ksu.edu.sa (M.S.A.); othaim@ksu.edu.sa (A.A.)

Abstract: Recently, there has been enormous development due to advancements in technology. Industries and enterprises are moving towards a digital system, and the oil and gas industries are no exception. There are several threats and risks in digital systems, which are controlled through cyber-security. For the first time in the theory of fuzzy sets, this research analyzes the relationships between cyber-security and cyber-crimes in the oil and gas sectors. The novel concepts of complex intuitionistic fuzzy relations (CIFRs) are introduced. Moreover, the types of CIFRs are defined and their properties are discussed. In addition, an application is presented that uses the Hasse diagram to make a decision regarding the most suitable cyber-security techniques to implement in an industry. Furthermore, the omnipotence of the proposed methods is explained by a comparative study.

1. Introduction

The techniques and methods used for reasoning, modeling and computing are mostly of precise, deterministic and crisp nature. The term crisp refers to the concept of a dichotomy, i.e., yes or no rather than more or less. In conventional dual logic, a statement is either true or false—there are no other possibilities. In general, precision implies that the models are unambiguous and clear. Crisp knowledge can be modeled using the crisp/classical set theory, also known as Cantor's set theory. Meanwhile, in mathematics, the uncertainty is modeled through the theory of fuzzy sets (FSs) and fuzzy logic (FL). In practice, uncertainty cannot be avoided. There have been numerous structures, techniques and formulations introduced to model uncertainty in the theory of FSs and FL. Each of these methods have their advantages, accompanied by some limitations, leaving some gaps. Thus, this paper focuses on the formulation of some novel structures and methods that aim to solve certain cyber-security and hacking issues faced by the oil and gas sectors.

The complex intuitionistic fuzzy set (CIFS) is a powerful tool in FS theory that is used to model ambiguity and uncertainty, but the concepts of relations have not yet been defined for CIFSs. This article introduces the concepts of relations in the theory of CIFSs. Using the Cartesian product of two CIFSs, the current study presents the definition of complex intuitionistic fuzzy relations (CIFRs). The formation of CIFSs is based on a pair of complex valued functions whose values and their sum are contained within the unit disc of a complex plane. These functions are called the membership grade and non-membership grade. The real portion of each of the complex valued functions is called the amplitude

term and the imaginary portion is called the phase term. This structure enables the CIFSs and their relations to model multidimensional problems of uncertain nature. These CIFRs generalize fuzzy relations (FRs), complex fuzzy relations (CFRs) and intuitionistic fuzzy relations (IFRs). By setting the non-membership grade to zero, the CIFR is converted into CFR. Similarly, by setting the phase terms equal to zero, the outcome is the IFRs and FRs. However, the converse is not true. Hence, the CIFRs are superior to their predecessors because they can also handle problems in fuzzy, intuitionistic fuzzy, complex fuzzy and complex intuitionistic fuzzy environments. Besides CIFRs, this article also defines numerous types of CIFRs, such as the converse of a CIFR, complex intuitionistic equivalence fuzzy relation, complex intuitionistic pre-order fuzzy relation, complex intuitionistic partial order fuzzy relation, complex intuitionistic total order fuzzy relation, complex intuitionistic strict order fuzzy relation, composition of complex intuitionistic equivalence fuzzy relations and complex intuitionistic fuzzy equivalence classes. Moreover, some interesting properties of CIFRs have been discussed. In addition, a few useful results regarding CIFRs and their subtypes have also been presented. Furthermore, the Hasse diagram for the complex intuitionistic partial order fuzzy relations and sets is introduced. Additionally, some important definitions related to the Hasse diagram have been presented—for instance, maximum, minimum, maximal, minimal, supremum, infimum, upper and lower bound elements. Every definition in the article is supported by a suitable example.

Over time, businesses, enterprises and industries are becoming digitalized because digital systems render the organizational operations and processes smoother, more efficient and less time-consuming. Although digital systems have improved productivity and reduced expenditures, they also place businesses and industries at great risk of cybercrimes. The oil and gas industries are also being digitalized and the history shows that there have been many cyberattacks in these industries. Hackers steal sensitive data and destroy stored data and personal information about employees, such as credit card data. To overcome these risks, certain cyber-security measures, methods, software and techniques have been developed and implemented. This article analyzes the relationships among some cyber-securities and cyber-threats in the oil and gas industries using the proposed concepts of CIFRs. An application is also presented that uses the complex intuitionistic partial order fuzzy relations to select the best possible cyber-security measures among all the available options, as well as the most suitable security technique among the short-listed ones. Thus, the current study provides some very useful mathematical modeling techniques that can solve very complex problems. A number of security methods have been introduced by experts, and this paper focuses on selecting the best security measures for an organization. This will not only save time and money, but also simplify the maintenance of the security systems. Moreover, it is necessary to adopt a specific security system to protect against some particular cyber-threats. Finally, a comparison is carried out among the proposed method and the existing methods.

The rest of the paper is organized in the following way:

Section 2 discusses the literature review of the study.

Section 3 reviews some predefined concepts, which play the role of building blocks for this article.

Section 4 is focused on CIFRs and their properties. Moreover, some results are provided, and Hasse diagrams and the related definitions are presented.

Section 5 proposes a couple of applications of the CIFRs to study the relationships among cyber-security and cyber-risks in the oil and gas industries.

Section 6 compares the proposed structure with the existing competitors.

Section 7 concludes the article.

2. Literature Review

Klir [1] devised the crisp relations that are used to study the relationships among the crisp sets. However, the modeling of ambiguity/uncertainty has long been a challenge for researchers. In 1965, Zadeh [2] introduced the fuzzy sets (FSs) and logics, which are capable

of modeling fuzziness, ambiguity and uncertainty. The elements of an FS are assigned a fuzzy function that takes values from the unit interval $[0, 1]$. This fuzzy function is called the membership grade, and the number from a unit interval is called the fuzzy number (FN). In fuzzy set theory, the statements are of the more or less type. Mendel [3] introduced the concept of fuzzy relations (FRs) that are used to analyze the relationships among the FSs. These relations are also characterized by membership grades whose values range between 0 and 1. Torra [4] introduced the hesitant FSs; Zadeh [5] presented the FSs as a basis for possibility theory; Negoita and Ralescu [6] applied the FSs to system analysis; Goguen [7] defined the L-FSs; and Laengle et al. [8] proposed a bibliometric analysis of FSs. Using genetic algorithm based on FSs, Xu et al. [9] optimized many-objective flow shop scheduling and Mewada et al. [10] extrapolated a fuzzy system with applications.

Ramot et al. [11] considered altering the membership grade and proposed the idea of complex fuzzy sets (CFSs). The elements of CFSs are assigned a complex fuzzy function that attains values from the unit circle in a complex plane. Obviously, the complex fuzzy function is called the membership grade, but here, a membership grade is a complex number, in contrast to a real number in FSs. Therefore, a complex membership grade has two parts: the amplitude term and phase term. These sets can model the ambiguity with phase changes and time periods. Furthermore, Ramot et al. [12] defined the complex fuzzy relations (CFRs) for CFSs; Pedrycz [13] worked on FRs and relational computing; Yu et al. [14] provided the uncertainty measures for FRs with applications; De Baets and Kerre [15] proposed the applications of FRs. Based on FRs, Tamura et al. [16] presented the pattern classification; Bhattacharya and Mukherjee [17] offered the FRs and fuzzy groups; Braae and Rutherford [18] used FRs in a control setting. Zhang et al. [19] introduced the operation properties and δ-equalities of CFSs; Yazdanbakhsh and Dick [20] systematically reviewed the CFSs and logic; Tamir et al. [21] presented an overview of CFSs and CF logic along with their applications; Ma et al. [22] proposed a method for multiple periodic factor prediction problems through CFSs, and Nasir et al. [23] used interval-valued CFRs in medical diagnosis and studied the lifespan of patients.

Zadeh's fuzzy set theory had a drawback in that it only discussed the membership grade, with only minor discussion of the non-membership grade, which is the complement of the membership grade, i.e., $1-$ membership grade. Therefore, Atanassov [24] defined the intuitionistic fuzzy sets (IFSs) that are characterized by a pair of functions called the membership and non-membership grades. Both of the grades attain values from the unit interval provided that their sum does not exceed 1. The numbers in the $[0, 1]$ interval that an IFS assigns to its grades are known as intuitionistic fuzzy numbers (IFNs). Burillo et al. [25] introduced the concepts of intuitionistic fuzzy relations (IFRs) for IFSs. These sets discuss the relationship in the environment of intuitionistic fuzzy set theory through the membership and non-membership grades. De et al. [26] applied IFSs in medical diagnosis; Szmidt and Kacprzyk [27] found the distances between IFSs; De et al. [28] defined some operations on IFSs; Gerstenkorn and Manko [29] gave the correlation of IFSs; Buyukozkan and Uzturk [30] used interval-valued IFQFD for designing a smart fridge; Rani and Garg [31] applied the CIFRs in individual and group decision-making problems; Bustince and Burillo [32] proposed structures on IFRs, and Deschrijver and Kerre [33] studied the composition of IFRs.

The involvement of complex numbers in IFSs was investigated by Alkouri et al. [34], who proposed the idea of complex intuitionistic fuzzy sets (CIFSs). A CIFS assigns each of its elements a pair of functions whose values are complex numbers from a unit circle provided that their sum also belongs to the unit circle in the complex plane. Similar to CFSs, the membership and non-membership grades of CIFSs also consist of amplitude terms and phase terms. Thus, they can model uncertain events with time periods and phase alterations. Yaqoob et al. [35] and Nasir et al. [36,37] studied the complex relations and applied them in cellular networks and economic relationships. Ngan et al. [38] represented CIFS by quaternion numbers and applied them in decision-making, while Kumar and Bajaj [39] worked on the distance measures and entropies in CIF soft sets.

The world is developing and every organization is being digitalized. This ensures that the operations of organizations are smooth, time-efficient, systematized and secure as compared to non-digital infrastructures. In recent years, hackers and other criminals have targeted the digital industries. There are certain threats and risks to the digital systems that need to be countered by implementing specific techniques. The oil and gas sectors are not an exception and have been targeted recently. Scientists and engineers have carried out research to make these industries secure. Lamba [40] described measures to protect the 'cybersecurity and resiliency' of the oil, energy and gas infrastructures of a nation; Line et al. [41] discussed the cyber-security challenges in smart grids; Lu et al. [42] and Lakhanpal and Samuel [43] reviewed the opportunities, applications, risks and challenges of implementing block-chain technology in oil and gas sectors. Based on factor state space, Yang et al. [44] presented a new cyber-security risk evaluation method; Stergiopoulos et al. [45] surveyed attack patterns and carried out incident assessment in the oil and gas industries to evaluate the cyber-attacks in the oil and gas sector; Wanasinghe et al. [46] carried out a systematic review of internet of things in the oil and gas sector, and Bjerga and Aven [47] used some new risk perspectives for adaptive risk management in the oil and gas sector.

3. Preliminaries

In this section, some fundamental concepts are reviewed, such as fuzzy sets (FSs), complex FSs (CFSs), intuitionistic FSs (CFSs), complex IFSs (CIFSs), Cartesian product (CP) of two CFSs and complex fuzzy relations (CFRs). In addition, the definitions are supported by examples.

Definition 1 ([2]). *An FS $\acute{I}$ is characterized by a function $m : \acute{I} \to [0,1]$ that assigns to each $u \in \acute{I}$ a fuzzy number (FN) $m(u) \in [0,1]$. The function m is called the membership grade. Henceforth, an FS $\acute{I}$ on a universal set $Ş$ is of the following form:*

$$\acute{I} = \Big\{ (u, m(u)) : u \in Ş \Big\}$$

Example 1. $\acute{I} = \{(u, 0.359), (v, 0.654), (w, 0.982), (x, 0.234), (y, 0.000), (z, 1.000)\}$ *is an FS.*

Definition 2 ([11]). *A CFS $\acute{I}$ is characterized by a function $m_C : \acute{I} \to \mathcal{Z}$, where $\mathcal{Z} \in \mathbb{C} \ni |\mathcal{Z}| \leq 1$. m_C assigns to each $u \in \acute{I}$ a complex number such that $|m_C(u)| \in [0,1]$. The function $m_C(u)$ is called the membership grade, defined as $m_C(u) = \alpha(u)e^{\rho(u)2\pi i}$, where $i = \sqrt{-1}$, $\alpha(u) \in [0,1]$ is named the amplitude term and $\rho(u) \in [0,1]$ is named the phase term. Henceforth, a CFS $\acute{I}$ on a universal set $Ş$ is of the following form:*

$$\acute{I} = \Big\{ \Big(u, \alpha(u)e^{\rho(u)2\pi i} \Big) : u \in Ş \Big\}$$

Example 2. $\acute{I} = \left\{ \begin{array}{l} \Big(u, 0.336e^{(0.526)2\pi i}\Big), \Big(v, 0.619e^{(0.736)2\pi i}\Big), \Big(w, 0.975e^{(0.128)2\pi i}\Big), \\ \Big(x, 0.254e^{(0.672)2\pi i}\Big), \Big(y, 0.000e^{(1.000)2\pi i}\Big), \Big(z, 1.000e^{(0.000)2\pi i}\Big) \end{array} \right\}$

is a CFS.

Definition 3 ([12]). *The CP of CFSs $\acute{I} = \left\{ \Big(u, \alpha^{\acute{I}}(u)e^{\rho^{\acute{I}}(u)2\pi i} \Big) : u \in Ş \right\}$ and*

$j = \left\{ \Big(v, \alpha^{j}(v)e^{\rho^{j}(v)2\pi i} \Big) : v \in Ş \right\}$ *is given by*

$$\acute{I} \times j = \left\{ \Big((u,v), \alpha^{\acute{I} \times j}(u,v)e^{\rho^{\acute{I} \times j}(u,v)2\pi i} \Big) : u \in \acute{I}, v \in j \right\}$$

where $\alpha^{\acute{I} \times j}(u,v) = \min\Big\{ \alpha^{\acute{I}}(u), \alpha^{j}(v) \Big\}$ and $\rho^{\acute{I} \times j}(u,v) = \min\Big\{ \rho^{\acute{I}}(u), \rho^{j}(v) \Big\}$.

Definition 4 ([12]). *Any subset of the CP of two CFSs is known as a complex fuzzy relation (CFR), which is symbolized by R.*

Example 3. *Let* $\acute{I} = \left\{ \left(u, 0.3e^{(0.5)2\pi i}\right), \left(v, 0.6e^{(0.7)2\pi i}\right), \left(w, 0.9e^{(0.1)2\pi i}\right) \right\}$ *and* $\jmath = \left\{ \left(x, 0.2e^{(0.6)2\pi i}\right), \left(y, 0e^{(1)2\pi i}\right), \left(z, 1e^{(0)2\pi i}\right) \right\}$, *then the CP is found to be*

$$\acute{I} \times \jmath = \left\{ \begin{array}{l} \left((u,x), 0.2e^{(0.5)2\pi i}\right), \left((u,y), 0e^{(0.5)2\pi i}\right), \left((u,z), 0.3e^{(0)2\pi i}\right), \\ \left((v,x), 0.2e^{(0.6)2\pi i}\right), \left((v,y), 0e^{(0.7)2\pi i}\right), \left((v,z), 0.6e^{(0)2\pi i}\right), \\ \left((w,x), 0.2e^{(0.1)2\pi i}\right), \left((w,y), 0e^{(0.1)2\pi i}\right), \left((w,z), 0.9e^{(0)2\pi i}\right) \end{array} \right\}$$

The CFR R is given as follows (Figure 1)

$$R = \left\{ \left((u,x), 0.2e^{(0.5)2\pi i}\right), \left((v,y), 0e^{(0.7)2\pi i}\right), \left((w,z), 0.9e^{(0)2\pi i}\right) \right\}$$
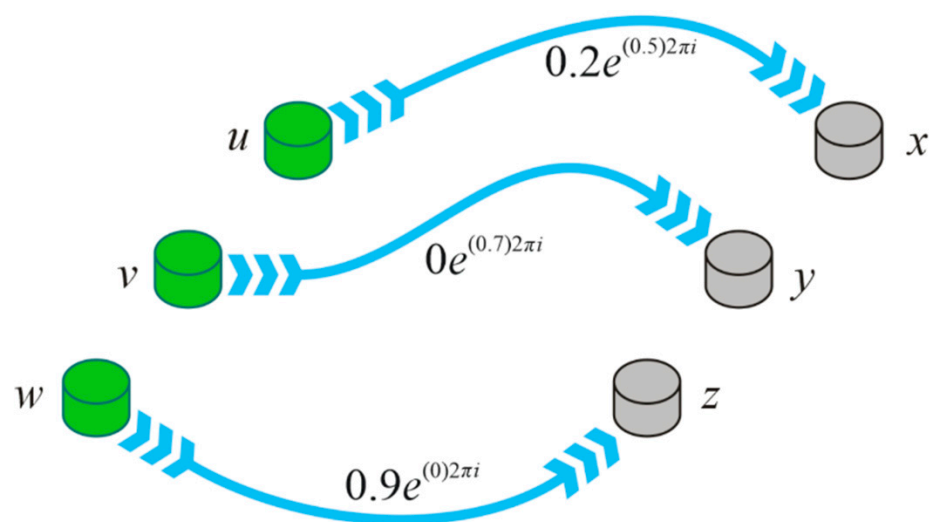

Figure 1. Complex fuzzy relation.

Definition 5 ([24]). *An IFS $\acute{I}$ is characterized by a pair of functions $m, n : \acute{I} \to [0,1]$ that are each assigned $u \in \acute{I}$ a pair of fuzzy numbers (FN) $m(u), n(u) \in [0,1]$, provided that the sum $m(u) + n(u) \leq 1$. The function m is called the membership grade and the function n is called the non-membership grade. Henceforth, an IFS $\acute{I}$ on a universal set $\mathcal{S}$ is of the following form*:

$$\acute{I} = \left\{ (u, m(u), n(u)) : u \in \mathcal{S} \right\}$$

Example 4. $\acute{I} = \{(u, 0.3, 0.5), (v, 0.6, 0.2), (w, 0.9, 0.1)\}$ *is an IFS.*

Definition 6 ([34]). *A CIFS $\acute{I}$ is characterized by a pair of complex valued functions $m_C, n_C : \acute{I} \to \mathcal{Z}$, where $\mathcal{Z} \, \epsilon \, \mathbb{C} \ni |\mathcal{Z}| \leq 1$. m_C and n_C assigns to each $u \in \acute{I}$ a pair of complex numbers such that $|m_C(u)|, |n_C(u)| \in [0,1]$ and $|m_C(u)| + |n_C(u)| \leq 1$. The function $m_C(u)$ is called the membership grade and the function $n_C(u)$ is called the non-membership grade, which are defined as $m_C(u) = \alpha_m(u)e^{\rho_m(u)2\pi i}$ and $n_C(u) = \alpha_n(u)e^{\rho_n(u)2\pi i}$, where $i = \sqrt{-1}$, $\alpha_m(u), \alpha_n(u) \in [0,1]$ are called the amplitude terms of the membership and non-membership grades, respectively, and $\rho_m(u), \rho_n(u) \in [0,1]$ are called the phase terms of the membership and non-membership grades, respectively. Henceforth, a CIFS $\acute{I}$ on a universal set $\mathcal{S}$ is of the following form*:

$$\acute{I} = \left\{ \left(u, \alpha_m(u)e^{\rho_m(u)2\pi i}, \alpha_n(u)e^{\rho_n(u)2\pi i}\right) : u \in \mathcal{S} \right\}$$

provided that $\alpha_m(u) + \alpha_n(u) \leq 1$ and $\rho_m(u) + \rho_n(u) \leq 1$.

Example 5. $\acute{I} = \left\{ \begin{array}{c} \left(u, 0.3e^{(0.5)2\pi i}, 0.3e^{(0.5)2\pi i}\right), \left(v, 0.5e^{(0.7)2\pi i}, 0.4e^{(0.2)2\pi i}\right), \\ \left(w, 0.1e^{(0.4)2\pi i}, 0.6e^{(0.6)2\pi i}\right) \end{array} \right\}$ *is a CIFS.*

4. Complex Intuitionistic Fuzzy Relations and Their Properties

This section introduces the novel concepts of CP of two CIFSs, complex intuitionistic fuzzy relations (CIFRs) and their types. Every definition is supported by a suitable example. Moreover, some interesting results for CIFRs are provided. Additionally, the Hasse diagram for the complex intuitionistic partial order relations is presented. The notions of maximum, minimum, maximal, minimal, supremum, infimum, upper and lower bounds are defined as well.

Definition 7. *The CP of CIFSs* $\acute{I} = \left\{ \left(u, \alpha_m^{\acute{I}}(u)e^{\rho_m^{\acute{I}}(u)2\pi i}, \alpha_n^{\acute{I}}(u)e^{\rho_n^{\acute{I}}(u)2\pi i}\right) : u \in \S \right\}$ *and* $\jmath = \left\{ \left(u, \alpha_m^{\jmath}(v)e^{\rho_m^{\jmath}(v)2\pi i}, \alpha_n^{\jmath}(v)e^{\rho_n^{\jmath}(v)2\pi i}\right) : v \in \S \right\}$ *is denoted and defined as*

$$\acute{I} \times \jmath = \left\{ \left((u,v), \alpha_m^{\acute{I} \times \jmath}(u,v)e^{\rho_m^{\acute{I} \times \jmath}(u,u)2\pi i}, \alpha_n^{\acute{I} \times \jmath}(u,v)e^{\rho_n^{\acute{I} \times \jmath}(u,v)2\pi i}\right) : u \in \acute{I}, v \in \jmath \right\}$$

where $\alpha_m^{\acute{I} \times \jmath}(u,v) = \min\left\{\alpha_m^{\acute{I}}(u), \alpha_m^{\jmath}(v)\right\}$, $\rho_m^{\acute{I} \times \jmath}(u,v) = \min\left\{\rho_m^{\acute{I}}(u), \rho_m^{\jmath}(v)\right\} \alpha_n^{\acute{I} \times \jmath}(u,v) = \max\left\{\alpha_n^{\acute{I}}(u), \alpha_n^{\jmath}(v)\right\}$ *and* $\rho_n^{\acute{I} \times \jmath}(u,v) = \max\left\{\rho_n^{\acute{I}}(u), \rho_n^{\jmath}(v)\right\}$.

Definition 8. *Any subset of the CP* $\acute{I} \times \jmath$ *of two CIFSs* $\acute{I}$ *and* $\jmath$ *is known as a complex intuitionistic fuzzy relation (CIFR) between* $\acute{I}$ *and* $\jmath$.

Any subset of the CP $\acute{I} \times \jmath$ *is known as a CIFR on* $\acute{I}$.
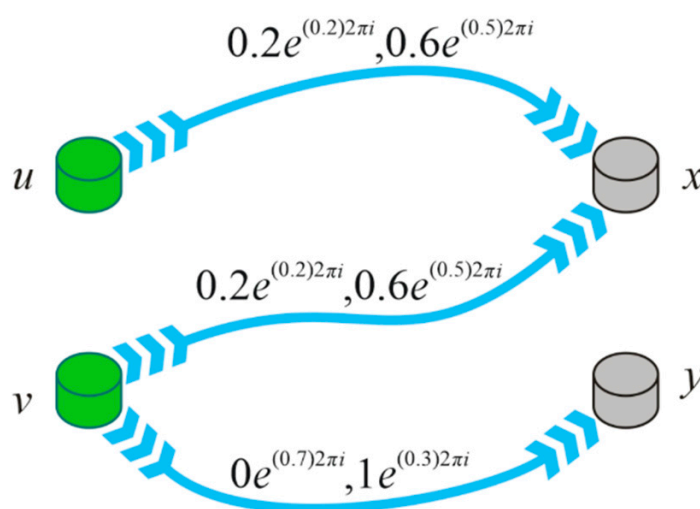*A CIFR is symbolized by R.*

Example 6. *Let* $\acute{I} = \left\{ \left(u, 0.3e^{(0.5)2\pi i}, 0.5e^{(0.4)2\pi i}\right), \left(v, 0.6e^{(0.7)2\pi i}, 0.4e^{(0.3)2\pi i}\right) \right\}$ *and* $\jmath = \left\{ \left(x, 0.2e^{(0.2)2\pi i}0.6e^{(0.5)2\pi i}\right), \left(y, 0e^{(1)2\pi i}, 1e^{(0)2\pi i}\right) \right\}$, *then the CP is found to be*

$$\acute{I} \times \jmath = \left\{ \begin{array}{c} \left((u,x), 0.2e^{(0.2)2\pi i}, 0.6e^{(0.5)2\pi i}\right), \left((u,y), 0e^{(0.5)2\pi i}, 1e^{(0.4)2\pi i}\right), \\ \left((v,x), 0.2e^{(0.2)2\pi i}, 0.6e^{(0.5)2\pi i}\right), \left((v,y), 0e^{(0.7)2\pi i}, 1e^{(0.3)2\pi i}\right) \end{array} \right\}$$

The CIFR R between $\acute{I}$ *and* $\jmath$ *is given as follows (Figure 2)*

$$R = \left\{ \begin{array}{c} \left((u,x), 0.2e^{(0.2)2\pi i}, 0.6e^{(0.5)2\pi i}\right), \left((v,x), 0.2e^{(0.2)2\pi i}, 0.6e^{(0.5)2\pi i}\right), \\ \left((v,y), 0e^{(0.7)2\pi i}, 1e^{(0.3)2\pi i}\right) \end{array} \right\}$$

Figure 2. Complex intuitionistic fuzzy relation.

NOTE: For convenience, (u, v) will be used to denote $\left((u, v), \alpha_m^{\acute{I} \times \acute{I}}(u, v) e^{\rho_m^{\acute{I} \times \acute{I}}(u, v) 2\pi i}, \alpha_n^{\acute{I} \times \acute{I}}(u, v) e^{\rho_n^{\acute{I} \times \acute{I}}(u, v) 2\pi i} \right)$ throughout this paper, unless otherwise stated.

Definition 9. *Let R be a CIFR on a CIFS $\acute{I}$. Then,*

1. *R is complex intuitionistic reflexive FR if $(u, u) \in R, \forall u \in \acute{I}$.*
2. *R is complex intuitionistic symmetric FR if $\forall u, v \in \acute{I}$.*

$$(u, v) \in R \Rightarrow (v, u) \in R.$$

3. *R is complex intuitionistic transitive FR if $\forall u, v, w \in \acute{I}$.*

$$(u, v) \in R \text{ and } (v, w) \in R \Rightarrow (u, w) \in R.$$

4. *A complex intuitionistic equivalence FR R on $\acute{I}$ possesses the following properties:*
   a. *Complex intuitionistic reflexive;*
   b. *Complex intuitionistic symmetric;*
   c. *Complex intuitionistic transitive.*

5. *A complex intuitionistic preorder FR R on $\acute{I}$ possesses the following properties:*
   a. *Complex intuitionistic reflexive;*
   b. *Complex intuitionistic transitive.*

6. *R is complex intuitionistic antisymmetric FR if $\forall u, v \in \acute{I}$.*

$$(u, v) \in R \text{ and } (v, u) \in R \Rightarrow u = v.$$

7. *A complex intuitionistic partial order FR R on $\acute{I}$ possesses the following properties:*
   a. *Complex intuitionistic reflexive;*
   b. *Complex intuitionistic antisymmetric;*
   c. *Complex intuitionistic transitive.*

   R is also called the complex intuitionistic order FR.

8. *R is complex intuitionistic complete FR if $\forall u, v \in \acute{I}$.*

$$(u, v) \in R \text{ or } (v, u) \in R.$$

9. *A complex intuitionistic linear order FR R on Í possesses the following properties*:

    a. *Complex intuitionistic reflexive;*
    b. *Complex intuitionistic antisymmetric;*
    c. *Complex intuitionistic transitive;*
    d. *Complex intuitionistic complete.*

    It is also called the complex intuitionistic total order FR.

10. *R is complex intuitionistic irreflexive FR if* $(u, u) \notin R, \forall u \in \acute{I}$.

11. *A complex intuitionistic strict order FR R on Í possesses the following properties*:

    a. *Complex intuitionistic irreflexive;*
    b. *Complex intuitionistic transitive.*

Example 7. *For a CIFS* $\acute{I} = \left\{ \begin{array}{l} \left(x, 0.20e^{(0.40)2\pi i}0.60e^{(0.50)2\pi i}\right), \\ \left(y, 0.10e^{(0.40)2\pi i}, 0.10e^{(0.30)2\pi i}\right), \\ \left(z, 0.60e^{(0.10)2\pi i}, 0.30e^{(0.80)2\pi i}\right) \end{array} \right\}$, *the CP* $\acute{I} \times \acute{I}$ *is found*

$$\acute{I} \times \acute{I} = \left\{ \begin{array}{l} \left((x,x), 0.20e^{(0.40)2\pi i}0.60e^{(0.50)2\pi i}\right), \left((x,y), 0.10e^{(0.40)2\pi i}0.60e^{(0.50)2\pi i}\right), \\ \left((x,z), 0.20e^{(0.10)2\pi i}0.60e^{(0.80)2\pi i}\right), \left((y,x), 0.10e^{(0.40)2\pi i}0.60e^{(0.50)2\pi i}\right), \\ \left((y,y), 0.10e^{(0.40)2\pi i}, 0.10e^{(0.30)2\pi i}\right), \left((y,z), 0.10e^{(0.10)2\pi i}0.30e^{(0.80)2\pi i}\right), \\ \left((z,x), 0.20e^{(0.10)2\pi i}0.60e^{(0.80)2\pi i}\right), \left((z,y), 0.10e^{(0.10)2\pi i}0.30e^{(0.80)2\pi i}\right), \\ \left((z,z), 0.60e^{(0.10)2\pi i}, 0.30e^{(0.80)2\pi i}\right) \end{array} \right\}$$

Then,

1. *The complex intuitionistic equivalence fuzzy relation* R_1 *on* $\acute{I} \times \acute{I}$ *is*

$$R_1 = \left\{ \begin{array}{l} \left((x,x), 0.20e^{(0.40)2\pi i}0.60e^{(0.50)2\pi i}\right), \left((x,y), 0.10e^{(0.40)2\pi i}0.60e^{(0.50)2\pi i}\right), \\ \left((y,x), 0.10e^{(0.40)2\pi i}0.60e^{(0.50)2\pi i}\right), \left((y,y), 0.10e^{(0.40)2\pi i}, 0.10e^{(0.30)2\pi i}\right), \\ \left((z,z), 0.60e^{(0.10)2\pi i}, 0.30e^{(0.80)2\pi i}\right) \end{array} \right\}$$

2. *The complex intuitionistic partial order fuzzy relation* R_2 *on* $\acute{I} \times \acute{I}$ *is*

$$R_2 = \left\{ \begin{array}{l} \left((x,x), 0.20e^{(0.40)2\pi i}0.60e^{(0.50)2\pi i}\right), \left((x,y), 0.10e^{(0.40)2\pi i}0.60e^{(0.50)2\pi i}\right), \\ \left((y,y), 0.10e^{(0.40)2\pi i}, 0.10e^{(0.30)2\pi i}\right), \left((z,y), 0.10e^{(0.10)2\pi i}0.30e^{(0.80)2\pi i}\right), \\ \left((z,z), 0.60e^{(0.10)2\pi i}, 0.30e^{(0.80)2\pi i}\right) \end{array} \right\}$$

3. *The complex intuitionistic linear order fuzzy relation* R_3 *on* $\acute{I} \times \acute{I}$ *is*

$$R_3 = \left\{ \begin{array}{l} \left((x,x), 0.20e^{(0.40)2\pi i}0.60e^{(0.50)2\pi i}\right), \left((x,y), 0.10e^{(0.40)2\pi i}0.60e^{(0.50)2\pi i}\right), \\ \left((x,z), 0.20e^{(0.10)2\pi i}0.60e^{(0.80)2\pi i}\right), \left((y,y), 0.10e^{(0.40)2\pi i}, 0.10e^{(0.30)2\pi i}\right), \\ \left((y,z), 0.10e^{(0.10)2\pi i}0.30e^{(0.80)2\pi i}\right), \left((z,z), 0.60e^{(0.10)2\pi i}, 0.30e^{(0.80)2\pi i}\right) \end{array} \right\}$$

4. *The complex intuitionistic strict order fuzzy relation* R_4 *on* $\acute{I} \times \acute{I}$ *is*

$$R_4 = \left\{ \begin{array}{l} \left((x,y), 0.10e^{(0.40)2\pi i}0.60e^{(0.50)2\pi i}\right), \left((x,z), 0.20e^{(0.10)2\pi i}0.60e^{(0.80)2\pi i}\right), \\ \left((y,z), 0.10e^{(0.10)2\pi i}0.30e^{(0.80)2\pi i}\right) \end{array} \right\}$$

Definition 10. *The converse of a CIFR R is defined as*

$$R^c = \{(v, u) : (u, v) \in R\}$$

Example 8. *For CIFSs*
$$\acute{I} = \left\{ \left(w, 0.4e^{(0.4)2\pi i}0.5e^{(0.5)2\pi i}\right), \left(x, 0.2e^{(0.4)2\pi i}0.6e^{(0.5)2\pi i}\right) \right\} \text{ and}$$
$$ȷ = \left\{ \left(y, 0.1e^{(0.4)2\pi i}, 0.1e^{(0.3)2\pi i}\right), \left(z, 0.6e^{(0.1)2\pi i}, 0.3e^{(0.8)2\pi i}\right) \right\}, \text{ the CP } \acute{I} \times ȷ \text{ is found}$$

$$R = \acute{I} \times ȷ = \left\{ \begin{array}{l} \left((w, y), 0.1e^{(0.4)2\pi i}0.5e^{(0.5)2\pi i}\right), \left((w, z), 0.4e^{(0.1)2\pi i}0.5e^{(0.8)2\pi i}\right), \\ \left((x, y), 0.1e^{(0.4)2\pi i}0.6e^{(0.5)2\pi i}\right), \left((x, z), 0.2e^{(0.1)2\pi i}0.6e^{(0.8)2\pi i}\right) \end{array} \right\}$$

Then, the converse of a CIFR R is given as

$$R^c = \left\{ \begin{array}{l} \left((y, w), 0.1e^{(0.4)2\pi i}0.5e^{(0.5)2\pi i}\right), \left((y, x), 0.1e^{(0.4)2\pi i}0.6e^{(0.5)2\pi i}\right), \\ \left((z, w), 0.4e^{(0.1)2\pi i}0.5e^{(0.8)2\pi i}\right), , \left((z, x), 0.2e^{(0.1)2\pi i}0.6e^{(0.8)2\pi i}\right) \end{array} \right\}$$

The complex intuitionistic equivalence fuzzy relations give rise to the concept of complex intuitionistic fuzzy equivalence classes, which are defined as follows.

Definition 11. *Let R be a complex intuitionistic equivalence fuzzy relation on a CIFS $\acute{I}$. For $u \in \acute{I}$, a complex intuitionistic fuzzy equivalence class of u mod R is defined and symbolized as*

$$R[u] = \{v | (v, u) \in R\}$$

Example 9. *For a CIFS* $\acute{I} = \left\{ \begin{array}{c} \left(x, 0.3e^{(0.4)2\pi i}0.5e^{(0.5)2\pi i}\right), \left(y, 0.4e^{(0.3)2\pi i}, 0.2e^{(0.3)2\pi i}\right), \\ \left(z, 0.8e^{(0.4)2\pi i}, 0.1e^{(0.6)2\pi i}\right) \end{array} \right\}$,
the CP $\acute{I} \times \acute{I}$ is found

$$\acute{I} \times \acute{I} = \left\{ \begin{array}{c} \left((x, x), 0.3e^{(0.4)2\pi i}0.5e^{(0.5)2\pi i}\right), \left((x, y), 0.3e^{(0.4)2\pi i}0.5e^{(0.5)2\pi i}\right), \\ \left((x, z), 0.3e^{(0.4)2\pi i}0.5e^{(0.6)2\pi i}\right), \left((y, x), 0.3e^{(0.4)2\pi i}0.5e^{(0.5)2\pi i}\right), \\ \left((y, y), 0.4e^{(0.3)2\pi i}, 0.2e^{(0.3)2\pi i}\right), \left((y, z), 0.4e^{(0.3)2\pi i}0.2e^{(0.6)2\pi i}\right), \\ \left((z, x), 0.3e^{(0.4)2\pi i}0.5e^{(0.6)2\pi i}\right), \left((z, y), 0.4e^{(0.3)2\pi i}0.2e^{(0.6)2\pi i}\right), \\ \left((z, z), 0.8e^{(0.4)2\pi i}, 0.1e^{(0.6)2\pi i}\right) \end{array} \right\}$$

The complex intuitionistic equivalence fuzzy relation on $\acute{I}$ is

$$R = \left\{ \begin{array}{c} \left((x, x), 0.3e^{(0.4)2\pi i}0.5e^{(0.5)2\pi i}\right), \left((x, y), 0.3e^{(0.4)2\pi i}0.5e^{(0.5)2\pi i}\right), \\ \left((y, x), 0.3e^{(0.4)2\pi i}0.5e^{(0.5)2\pi i}\right), \left((y, y), 0.4e^{(0.3)2\pi i}, 0.2e^{(0.3)2\pi i}\right), \\ \left((z, z), 0.8e^{(0.4)2\pi i}, 0.1e^{(0.6)2\pi i}\right) \end{array} \right\}$$

Then, the complex intuitionistic fuzzy equivalence class of
1.   *x mod R is*

$$R[x] = \left\{ \left(x, 0.3e^{(0.4)2\pi i}0.5e^{(0.5)2\pi i}\right), \left(y, 0.4e^{(0.3)2\pi i}, 0.2e^{(0.3)2\pi i}\right) \right\}$$

2.   *y mod R is*

$$R[y] = \left\{ \left(x, 0.3e^{(0.4)2\pi i}0.5e^{(0.5)2\pi i} \right), \left(y, 0.4e^{(0.3)2\pi i}, 0.2e^{(0.3)2\pi i} \right) \right\}$$

3.   *z mod R is*

$$R[z] = \left\{ \left(z, 0.8e^{(0.4)2\pi i}, 0.1e^{(0.6)2\pi i} \right) \right\}$$

Definition 12. *Let R be a CIFR on a CIFS Í. Then, the complex intuitionistic composite FR $R \circ R$ is defined as*
For any $(u, v) \in R$ and $(v, w) \in R \Rightarrow (u, w) \in R \circ R, \forall u, v, w \in U$.

Example 10.   *Let R_1 and R_2 be two CIFRs on some CIFS Í $=$*
$\left\{ \left(x, 0.3e^{(0.4)2\pi i}0.5e^{(0.5)2\pi i} \right), \left(y, 0.4e^{(0.3)2\pi i}, 0.2e^{(0.3)2\pi i} \right), \left(z, 0.8e^{(0.4)2\pi i}, 0.1e^{(0.6)2\pi i} \right) \right\}$,

$$R_1 = \left\{ \begin{array}{c} \left((x,y), 0.3e^{(0.4)2\pi i}0.5e^{(0.5)2\pi i} \right), \left((y,y), 0.4e^{(0.3)2\pi i}, 0.2e^{(0.3)2\pi i} \right) \\ \left((z,z), 0.8e^{(0.4)2\pi i}, 0.1e^{(0.6)2\pi i} \right) \end{array} \right\}$$

$$R_2 = \left\{ \begin{array}{c} \left((x,z), 0.3e^{(0.4)2\pi i}0.5e^{(0.6)2\pi i} \right), \left((y,x), 0.3e^{(0.4)2\pi i}0.5e^{(0.5)2\pi i} \right), \\ \left((z,y), 0.4e^{(0.3)2\pi i}0.2e^{(0.6)2\pi i} \right) \end{array} \right\}$$

Then, the complex intuitionistic composite fuzzy relation $R_1 \circ R_2$ is given by

$$R_1 \circ R_2 = \left\{ \begin{array}{c} \left((x,x), 0.3e^{(0.4)2\pi i}0.5e^{(0.5)2\pi i} \right), \left((y,x), 0.3e^{(0.4)2\pi i}0.5e^{(0.5)2\pi i} \right), \\ \left((z,y), 0.4e^{(0.3)2\pi i}0.2e^{(0.6)2\pi i} \right) \end{array} \right\}$$

Theorem 1. *The CIFR R is a complex intuitionistic symmetric FR on a CIFS Í iff $R = R^c$.*

Proof. Let $R = R^c$, then

$$(u, v) \in R \Leftrightarrow (v, u) \in R^c \Leftrightarrow (v, u) \in R$$

Hence, R is a complex intuitionistic symmetric FR on a CIFS Í.
Conversely, suppose that R is a complex intuitionistic symmetric FR on a CIFS Í, then

$$(u, v) \in R \Leftrightarrow (v, u) \in R$$

However, $(v, u) \in R^c \Rightarrow R = R^c$. □

Theorem 2. *The CIFR $\mathcal{R}$ is a complex intuitionistic transitive FR on a CIFS Í iff $R \circ R \subseteq R$.*

Proof. Let R is a complex intuitionistic transitive FR on a CIFS Í. Assume that

$$(u, w) \in R \circ R$$

then, by the transitivity of R,

$$(u, v) \in R \text{ and } (v, w) \in R \Rightarrow (u, w) \in R \Rightarrow R \circ R \subseteq R.$$

Conversely, suppose that $R \circ R \subseteq R$; then, for

$$(u, v) \in R \text{ and } (v, w) \in R \Rightarrow (u, w) \in R \circ R \subseteq R \Rightarrow (u, w) \in R.$$

Hence, R is complex intuitionistic transitive FR on $\acute{Í}$. $\square$

Theorem 3. *If R is a complex intuitionistic equivalence FR on a CIFS $\acute{Í}$, then $R \circ R = R$.*

Proof. Let $(u, v) \in R$
Then, by the symmetry of a complex intuitionistic equivalence FR R,

$$(v, u) \in R$$

Now, by using the transitive property of a complex intuitionistic equivalence FR R,

$$(u, u) \in R$$

However, by the definition of complex intuitionistic composite FR,

$$(u, u) \in R \circ R$$

$$\text{Thus } R \subseteq R \circ R. \tag{1}$$

Conversely, suppose that $(u, v) \in R \circ R$, then $\exists \, w \in U \ni (u, w) \in R$ and $(w, v) \in R$
However, since R is a complex intuitionistic equivalence FR on $\acute{Í}$, R is also a complex intuitionistic transitive FR. Thus,

$$(u, v) \in R \Rightarrow R \circ R \subseteq R \tag{2}$$

Hence, by (1) and (2),

$$R \circ R = R.$$

$\square$

Theorem 4. *The converse of a complex intuitionistic partial order FR R on a CIFS $\acute{Í}$ is also a complex intuitionistic partial order FR on $\acute{Í}$.*

Proof. In order to prove the assertion, it is sufficient to show that the converse of a complex intuitionistic partial order FR R^c satisfies the three properties of a complex intuitionistic partial order FR.

i   Since R is a complex intuitionistic reflexive FR. Thus, for some $u \in U$,

$$(u, u) \in R \Rightarrow (u, u) \in R^c$$

Hence, $\mathcal{R}^c$ is a complex intuitionistic reflexive FR.

ii   Let $(u, u) \in R^c$ and $(v, u) \in R^c$

$$\text{Then } (u, v) \in R \text{ and } (v, u) \in R$$

However, R is a complex intuitionistic anti-symmetric FR. Thus,

$$(u, v) = (v, u)$$

Therefore, R^c is also a complex intuitionistic anti-symmetric FR.

iii   Let $(u, v) \in R^c$ and $(v, w) \in R^c$

$$\text{Then } (w, v) \in R \text{ and } (v, u) \in R$$

However, since R is a complex intuitionistic transitive FR. Thus,

$$(w, u) \in R \Rightarrow (u, w) \in R^c.$$

Thus, R^c is also a complex intuitionistic transitive FR.

From i, ii and iii, it is proven that R^c is also a complex intuitionistic partial order FR. □

Theorem 5. *If R is a complex intuitionistic equivalence FR on a CIFS* Í́, *then* $(u, v) \in R,$ *iff* $R[u] = R[v].$

Proof. Let $(u, v) \in R$ and $w \in R[u] \Rightarrow (w, u) \in R$.

Now, by the transitive property of R,

$$(w, v) \in R \Rightarrow w \in R[v]. \tag{3}$$

Therefore, $R[u] \subseteq R[v].$

Since $(u, v) \in R$, by using the symmetric property of R

$$(v, u) \in R.$$

Moreover, suppose that $w \in R[v] \Rightarrow (w, v) \in R$.

Now, by the transitive property of R,

$$(w, u) \in R \Rightarrow w \in R[u]. \tag{4}$$

Therefore, $R[v] \subseteq R[u].$

Hence, (3) and (4) imply that $R[v] = R[u].$

Conversely, let $R[v] = R[u], w \in R[u]$ and $w \in R[v] \Rightarrow (w, v) \in R$ and $(w, u) \in R$ Using the symmetric property of R

$$(w, u) \in R \Rightarrow (u, w) \in R$$

Now, by the transitive property of R, $(u, w) \in R$ and $(w, v) \in R \Rightarrow (u, v) \in R$, which completes the proof. □

Definition 13. *A pictorial delineation of the partial order relation is called a Hasse diagram. It consists of dots and line segments known as vertices and edges, respectively. A Hasse diagram does not have self-loops but directional and redundant edges. Each element of the set is represented by a vertex and the relationship among them is represented through edges that join these vertices according to the following rules:*

a. *The elements are arranged in an order or ranked up and down based on their relationships. The elements that are related to all other elements are kept at the bottom and the elements to whom every element of the set is related are kept at the top.*

b. *Two vertices are joined by an edge if and only if they are related to each other.*

Example 11. *Let us draw a Hasse diagram of the complex intuitionistic partial order FR R on a*

$$CIFS \, Í = \left\{ \begin{array}{c} \left(p, 0.31e^{(0.52)2\pi i}, 0.53e^{(0.44)2\pi i} \right), \left(q, 0.65e^{(0.76)2\pi i}, 0.27e^{(0.18)2\pi i} \right), \\ \left(r, 0.29e^{(0.40)2\pi i}, 0.61e^{(0.52)2\pi i} \right), \left(s, 0.13e^{(0.44)2\pi i}, 0.15e^{(0.36)2\pi i} \right), \\ \left(t, 0.67e^{(0.18)2\pi i}, 0.12e^{(0.80)2\pi i} \right) \end{array} \right\},$$

The CP is found to be

$$
\acute{I} \times \acute{I} = \left\{
\begin{array}{l}
\left((p,p),0.31e^{(0.52)2\pi i},0.53e^{(0.44)2\pi i}\right), \left((p,q),0.31e^{(0.52)2\pi i},0.53e^{(0.44)2\pi i}\right), \\
\left((p,r),0.29e^{(0.40)2\pi i},0.61e^{(0.52)2\pi i}\right), \left((p,s),0.13e^{(0.44)2\pi i},0.53e^{(0.44)2\pi i}\right), \\
\left((p,t),0.31e^{(0.18)2\pi i},0.53e^{(0.80)2\pi i}\right), \left((q,p),0.31e^{(0.52)2\pi i},0.53e^{(0.44)2\pi i}\right), \\
\left((q,q),0.65e^{(0.76)2\pi i},0.27e^{(0.18)2\pi i}\right), \left((q,r),0.29e^{(0.40)2\pi i},0.61e^{(0.52)2\pi i}\right), \\
\left((q,s),0.13e^{(0.44)2\pi i},0.27e^{(0.18)2\pi i}\right), \left((q,t),0.67e^{(0.18)2\pi i},0.27e^{(0.80)2\pi i}\right), \\
\left((r,p),0.29e^{(0.40)2\pi i},0.61e^{(0.52)2\pi i}\right), \left((r,q),0.29e^{(0.40)2\pi i},0.61e^{(0.52)2\pi i}\right), \\
\left((r,r),0.29e^{(0.40)2\pi i},0.61e^{(0.52)2\pi i}\right), \left((r,s),0.13e^{(0.40)2\pi i},0.61e^{(0.52)2\pi i}\right), \\
\left((r,t),0.29e^{(0.18)2\pi i},0.61e^{(0.80)2\pi i}\right), \left((s,p),0.13e^{(0.44)2\pi i},0.53e^{(0.44)2\pi i}\right), \\
\left((s,q),0.13e^{(0.44)2\pi i},0.27e^{(0.18)2\pi i}\right), \left((s,r),0.13e^{(0.40)2\pi i},0.61e^{(0.52)2\pi i}\right), \\
\left((s,s),0.13e^{(0.44)2\pi i},0.15e^{(0.36)2\pi i}\right), \left((s,t),0.13e^{(0.18)2\pi i},0.15e^{(0.80)2\pi i}\right), \\
\left((t,p),0.31e^{(0.18)2\pi i},0.53e^{(0.80)2\pi i}\right), \left((t,q),0.67e^{(0.18)2\pi i},0.27e^{(0.80)2\pi i}\right), \\
\left((t,r),0.29e^{(0.18)2\pi i},0.61e^{(0.80)2\pi i}\right), \left((t,s),0.13e^{(0.18)2\pi i},0.15e^{(0.80)2\pi i}\right), \\
\left((t,t),0.67e^{(0.18)2\pi i},0.12e^{(0.80)2\pi i}\right)
\end{array}
\right\}
$$

A complex intuitionistic partial order FR R is

$$
R = \left\{
\begin{array}{l}
\left((p,p),0.31e^{(0.52)2\pi i},0.53e^{(0.44)2\pi i}\right), \left((p,q),0.31e^{(0.52)2\pi i},0.53e^{(0.44)2\pi i}\right), \\
\left((p,r),0.29e^{(0.40)2\pi i},0.61e^{(0.52)2\pi i}\right), \left((p,s),0.13e^{(0.44)2\pi i},0.53e^{(0.44)2\pi i}\right), \\
\left((p,t),0.31e^{(0.18)2\pi i},0.53e^{(0.80)2\pi i}\right), \left((q,q),0.65e^{(0.76)2\pi i},0.27e^{(0.18)2\pi i}\right), \\
\left((q,s),0.13e^{(0.44)2\pi i},0.27e^{(0.18)2\pi i}\right), \left((q,t),0.67e^{(0.18)2\pi i},0.27e^{(0.80)2\pi i}\right), \\
\left((r,q),0.29e^{(0.40)2\pi i},0.61e^{(0.52)2\pi i}\right), \left((r,r),0.29e^{(0.40)2\pi i},0.61e^{(0.52)2\pi i}\right), \\
\left((r,s),0.13e^{(0.40)2\pi i},0.61e^{(0.52)2\pi i}\right), \left((r,t),0.29e^{(0.18)2\pi i},0.61e^{(0.80)2\pi i}\right), \\
\left((s,s),0.13e^{(0.44)2\pi i},0.15e^{(0.36)2\pi i}\right), \left((s,t),0.13e^{(0.18)2\pi i},0.15e^{(0.80)2\pi i}\right), \\
\left((t,t),0.67e^{(0.18)2\pi i},0.12e^{(0.80)2\pi i}\right)
\end{array}
\right\}
$$

Figure 3 displays the Hasse diagram of R.

p	$0.31e^{(0.52)2\pi i},0.53e^{(0.44)2\pi i}$
q	$0.65e^{(0.76)2\pi i},0.27e^{(0.18)2\pi i}$
r	$0.29e^{(0.40)2\pi i},0.61e^{(0.52)2\pi i}$
s	$0.13e^{(0.44)2\pi i},0.15e^{(0.36)2\pi i}$
t	$0.67e^{(0.18)2\pi i},0.12e^{(0.80)2\pi i}$

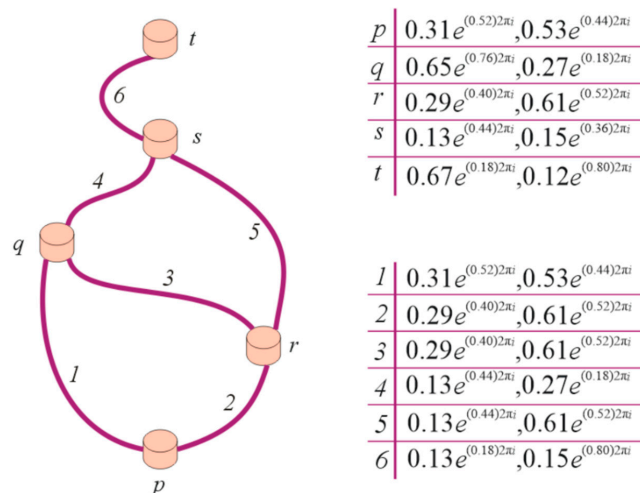|	
1	$0.31e^{(0.52)2\pi i},0.53e^{(0.44)2\pi i}$
2	$0.29e^{(0.40)2\pi i},0.61e^{(0.52)2\pi i}$
3	$0.29e^{(0.40)2\pi i},0.61e^{(0.52)2\pi i}$
4	$0.13e^{(0.44)2\pi i},0.27e^{(0.18)2\pi i}$
5	$0.13e^{(0.44)2\pi i},0.61e^{(0.52)2\pi i}$
6	$0.13e^{(0.18)2\pi i},0.15e^{(0.80)2\pi i}$

Figure 3. Hasse diagram for *R*.

Definition 14. *An element*

1. *That succeeds all the other elements is known as the maximum or greatest element.*
2. *That precedes all the other elements is known as the minimum or least element.*
3. *That is not related to any other element is known as the maximal element. The topmost elements of the Hasse diagram are the maximal elements.*
4. *To whom any other element(s) is(are) not related is(are) known as the minimal element(s). In other words, the element(s) that is(are) related to every other element is(are) the minimal element(s). The bottommost elements of the Hasse diagram are the minimal elements.*

Example 12. *Let* $\{p, q, r, s, t, u, v, w, x, y, z\}$ *be the elements of a complex intuitionistic partial order fuzzy set* Í. *For convenience, we ignore the membership and non-membership grades. Figure 4 shows the Hasse diagram of set* Í.
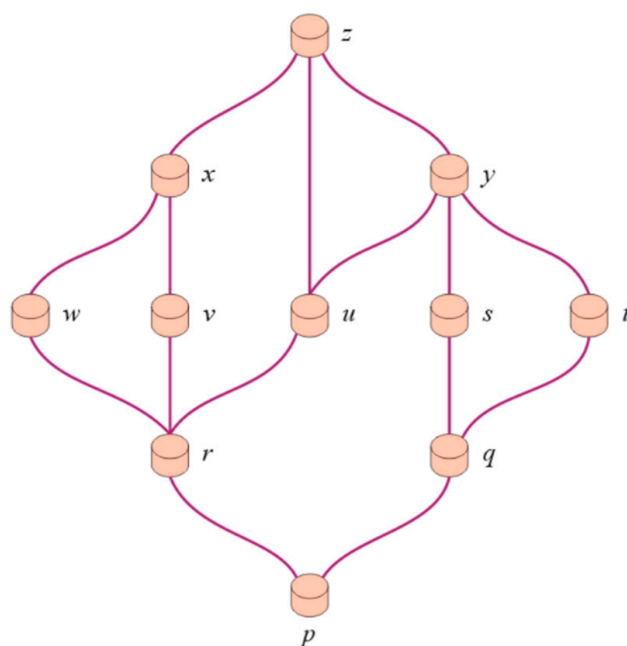
Figure 4. Hasse diagram for maximum, maximal, minimum and minimal elements.

*In the above diagram, z is the maximum and maximal element, while p is the minimum and minimal element.*

Definition 15. *For a subset* ȷ *of* Í, *an element* $u \in R \subseteq Í \times Í$ *is known as the*

1. *upper bound of* ȷ *if* $(v, u) \in R, \ \forall v \in ȷ$.
2. *lower bound of* ȷ *if* $(u, v) \in R, \ \forall v \in ȷ$.

Definition 16. *Let* ȷ *be a subset of a CIFS* Í, *then the least upper bound and the greatest lower bound of* ȷ *are called the supremum and infimum of* ȷ, *respectively.*

Example 13. *Let* $\{p, q, r, s, t, u, v, w, x, y, z\}$ *be the elements of a complex intuitionistic partial order fuzzy set* Í *and* $ȷ = \{q, r, s, t, u, y\}$ *be a subset of* Í. *For convenience, we ignore the membership and non-membership grades. Figure 5 shows the Hasse diagram of set* ȷ. *The elements of set* Í *are colored blue.*
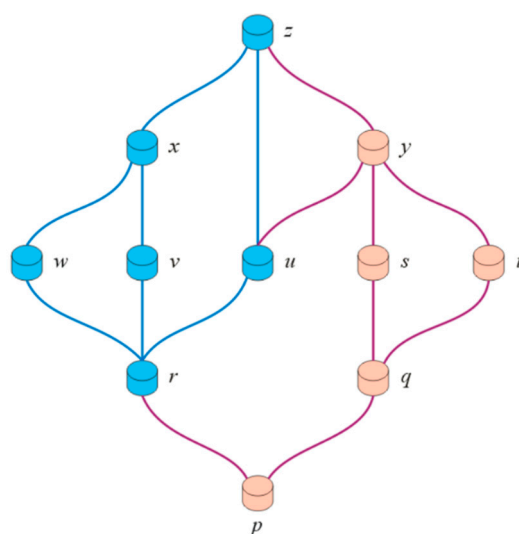
**Figure 5.** Hasse diagram for upper and lower bounds, supremum and infimum.

In the above diagram, y and z are the upper bounds of ꞁ, whereas, y is the supremum of ꞁ.
On the other hand, p and r are the lower bound of ꞁ, while r is the infimum of ꞁ.

5. Application

This section presents a couple of applications of the proposed concepts in the fields of information technology; more specifically, we consider cyber-security and cyber-crimes in the oil and gas industries.

5.1. Cyber-Security in Oil and Gas Industries

Huge development and modernization has taken place as a result of digitalization among various industries, and the oil and gas sector is no exception. Although advanced technological solutions such as IIOT (Industrial Internet of Things) have improved efficiency and reduced industrial expenditures, they have also exposed the oil and gas industries to the risks of cyber-crimes. These threats can have severely negative impacts on the company, resulting in massive losses of money and reputation and leading to environmental disasters. Below are some threats and the methods used for security purposes by an oil and gas company. Figure 6 presents the flowchart for the process followed in the application.
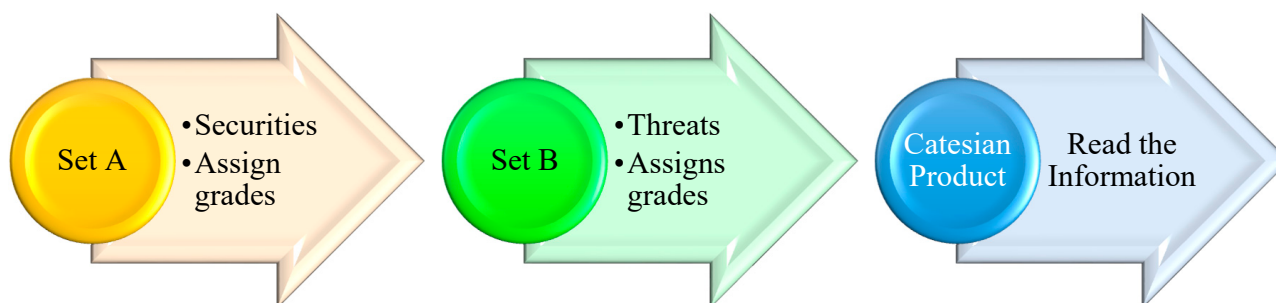
Figure 6. Flowchart for the process being followed.

5.1.1. Threats

Some of the threats that an oil and gas company are vulnerable to are explained below. Moreover, each threat and malware has been assigned the membership and non-membership grades. These membership grades are set by professionals according to their performance and operation. The membership grade for a threat indicates its weakness,

while the non-membership grade shows the strength or the severity of the threat. Since the grades range between 0 and 1, in the case of the membership grade, values closer to 1 represent greater effectiveness or success in accomplishing the target, while lower values i.e., close to zero, indicate less effectiveness and success in accomplishing the target. On the other hand, higher values of the non-membership grade indicate a higher likelihood of failure in achieving the goals and vice versa. Table 1 summarizes this section. The amplitude term represents the level of strength or weakness, while the phase term refers to the timeframe. In addition, higher values of the phase terms reflect a greater time period and the lower values refer to a shorter timespan.

Table 1. Summary of threats.

Threat	Abbreviation	Weakness Level	Threat Level
Infrastructure sabotage	IS	$0.4e^{(0.5)\pi i}$	$0.5e^{(0.5)\pi i}$
Espionage and data theft	$E\&DT$	$0.5e^{(0.6)\pi i}$	$0.5e^{(0.2)\pi i}$
Ever-changing malware	ECM	$0.4e^{(0.4)\pi i}$	$0.6e^{(0.5)\pi i}$
Ransomware	RW	$0.6e^{(0.7)\pi i}$	$0.4e^{(0.2)\pi i}$
Insider threat	InT	$0.4e^{(0.3)\pi i}$	$0.6e^{(0.6)\pi i}$

a. Infrastructure sabotage (IS): Cyber-criminals deploy malware and viruses that are specifically used to sabotage the networks, control systems or servers. The oil and gas industries have been attacked by different types of wiper malwares, such as Stuxnet malware and Industroyer.

$$\left(IS,\ 0.4e^{(0.5)\pi i}, 0.5e^{(0.5)\pi i} \right)$$

b. Espionage and data theft ($E\&DT$) are very serious concerns. Industries and companies are highly dependent on unique information that keeps them ahead of their competitors. In the oil and gas sector, data such as experimental results, boring procedures, new oil reserves and the chemistry of top products are extremely valuable. Thus, such data carry the greatest risk. Some tactics used for such attacks include DNS hijacking, phishing emails and corporate VPN servers or even scraping information that is openly available to obtain data.

$$\left(E\&DT,\ 0.5e^{(0.6)\pi i}, 0.5e^{(0.2)\pi i} \right)$$

c. Ever-changing malware (ECM): Usually, there are different malwares that are executed to fulfil different purposes, such as intrusion, data theft, propagation, etc. A cyber-criminal wishes to maintain their access to the targeted system in order to steal critical information by continuously and constantly updating the malware codes. Some malwares used by cyber-criminals to infect targets, maintain persistence and communicate are web-shells, DNS tunneling, email and cloud services.

$$\left(ECM,\ 0.4e^{(0.4)\pi i}, 0.6e^{(0.5)\pi i} \right)$$

d. Ransomware (RW) is a malware that is used to steal or encode the valuable information of a company. These malwares hugely impact the regular operations of an industry. In order to recover lost data, the industries are more likely to pay the ransom.

$$\left(RW,\ 0.6e^{(0.7)\pi i}, 0.4e^{(0.2)\pi i} \right)$$

e.　Insider threat (InT) is a serious threat to an industry that comes from the employees, former employees, contractors or business associates of the industry, i.e., people with confidential information about security practices, data and the digital system.

$$\left(InT, 0.4e^{(0.3)\pi i}, 0.6e^{(0.6)\pi i} \right)$$

Henceforth, the CIFS ⅉ summarizing the security threats is given below:

$$\jmath = \left\{ \begin{array}{c} \left(IS,\ 0.4e^{(0.5)\pi i}, 0.5e^{(0.5)\pi i} \right), \left(E\&DT,\ 0.5e^{(0.6)\pi i}, 0.5e^{(0.2)\pi i} \right), \\ \left(ECM,\ 0.4e^{(0.4)\pi i}, 0.6e^{(0.5)\pi i} \right), \left(RW,\ 0.6e^{(0.7)\pi i}, 0.4e^{(0.2)\pi i} \right), \\ \left(InT, 0.4e^{(0.3)\pi i}, 0.6e^{(0.6)\pi i} \right) \end{array} \right\}$$

5.1.2. Security Methods

The methods, techniques and practices adopted by the oil and gas industries to protect against cyber-crimes are discussed below. Each security method is assigned a pair of functions in the form of membership and non-membership grades. The membership grade represents the security level of a method, while the non-membership grade represents the risk levels that can result from implementing these techniques. Table 2 recaps this section. The amplitude term refers to the level or grade of security or risk, while the phase term refers to time. The assignation of the values the phase terms and amplitude term of membership and non-membership grades is similar to the assignment of values to the threats. Obviously, greater values of amplitude terms of membership grades are preferable with regard to security because they indicate greater security. However, higher values of phase terms of membership grades are also important, as they indicate long-term security. On the contrary, smaller values of amplitude terms of non-membership grades refer to a lower risk or insecurity. Thus, better security is indicated by a greater amplitude term value as well as a greater phase term value of its membership grade and lower values of the amplitude term and phase term of non-membership grades. Some of the most important security methods for the oil and gas industry are defined below with their fuzzy grades.

Table 2. Summary of security measures.

Security Method	Abbreviation	Security Level	Risk Level
Deep Armor Industrial	DMI	$0.7e^{(0.8)\pi i}$	$0.1e^{(0.2)\pi i}$
Event Monitoring	EM	$0.6e^{(0.6)\pi i}$	$0.3e^{(0.3)\pi i}$
Cyber-security workplace	CSW	$0.6e^{(0.4)\pi i}$	$0.2e^{(0.4)\pi i}$
Nozomi Network solution	NNS	$0.5e^{(0.5)\pi i}$	$0.3e^{(0.4)\pi i}$
Forge Cyber-Security Suite	FCS	$0.5e^{(0.4)\pi i}$	$0.2e^{(0.4)\pi i}$
Managed Security Services	MSS	$0.4e^{(0.5)\pi i}$	$0.4e^{(0.2)\pi i}$

a.　Deep Armor Industrial (DMI) is an AI-based technology that identifies and reports new devices or irregular activities such as insider threats and digital–physical attacks. Due to its predictive analysis, the execution of malicious codes is prevented. It is highly effective and can stop codes that are not yet present in threat intelligence packages. DMI provides unique, innovative and exceptional security to the oil and gas industries, even against new threats that emerge between updates, or cyber-attacks that arrive at isolated sites before patches can be deployed. It intends to provide the latest antivirus software, detection of threats, control of application and zero-day attack prevention to the industry.

$$\left(DMI,\ 0.7e^{(0.8)\pi i}, 0.1e^{(0.2)\pi i} \right)$$

b. ABB's Event Monitoring (*EM*) is a cyber-security solution that enables the security teams to more effectively identify, rank and react to threats across an OT network. Consecutively, it aids in the mitigation of risks significantly. Moreover, it eliminates the manual monitoring tasks, which saves the time in the process of threat detection. Thus, the customers can focus on value-added tasks.

$$\left(EM, \ 0.6e^{(0.6)\pi i}, 0.3e^{(0.3)\pi i} \right)$$

c. ABB's cyber-security workplace (*CSW*) is another innovative solution that enables companies to automatically and securely perform maintenance and routine tasks for their plant, without affecting the safety. It also offers the control and tracking of security patches, backup frequency and critical hardening measures.

$$\left(CSW, \ 0.6e^{(0.4)\pi i}, 0.2e^{(0.4)\pi i} \right)$$

d. Nozomi network solution (*NNS*) is an innovative cyber-security solution that provides greater threat detection, accurate asset discovery and flexible and scalable deployment. It also provides superior operational visibility and OT cyber-security.

$$\left(NNS, \ 0.5e^{(0.5)\pi i}, 0.3e^{(0.4)\pi i} \right)$$

e. Forge Cyber-Security Suite (*FCS*) is a strong software solution that is used by the oil and gas industries to simplify, strengthen and scale the industrial cyber-security operations when facing evolving threats.

$$\left(FCS, \ 0.5e^{(0.4)\pi i}, 0.2e^{(0.4)\pi i} \right)$$

f. Managed Security Services (*MSS*) proactively monitors, measures and manages industrial cyber-security risk.

$$\left(MSS, \ 0.4e^{(0.5)\pi i}, 0.4e^{(0.2)\pi i} \right)$$

Henceforth, the following CIFS $\acute{\text{Í}}$ summarizing the security methods is constructed:

$$\acute{\text{Í}} = \left\{ \begin{array}{l} \left(DMI, \ 0.7e^{(0.8)\pi i}, 0.1e^{(0.2)\pi i} \right), \left(EM, \ 0.6e^{(0.6)\pi i}, 0.3e^{(0.3)\pi i} \right), \\ \left(CSW, \ 0.6e^{(0.4)\pi i}, 0.2e^{(0.4)\pi i} \right), \left(NNS, \ 0.5e^{(0.5)\pi i}, 0.3e^{(0.4)\pi i} \right), \\ \left(FCS, \ 0.5e^{(0.4)\pi i}, 0.2e^{(0.4)\pi i} \right), \left(MSS, \ 0.4e^{(0.5)\pi i}, 0.4e^{(0.2)\pi i} \right) \end{array} \right\}$$

5.1.3. Calculations

Here, in order to study the relationships among the effectiveness and incompetency of each cyber-security technique against every cyber-crime, we carry out the following mathematics.

We have the following two CIFSs $\acute{\text{Í}}$ and j representing the set of securities and the set of threats, respectively.
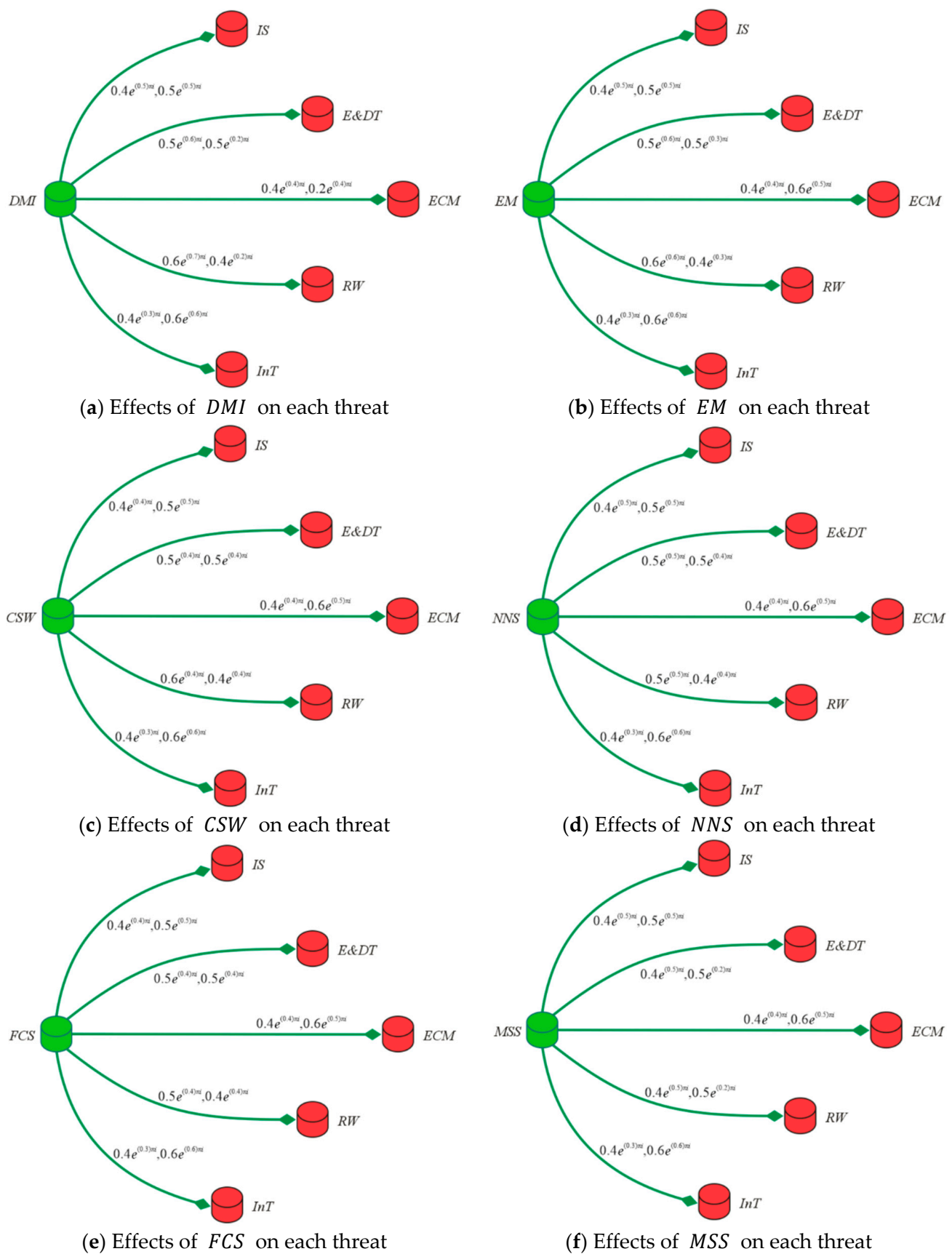
$$\acute{\text{Í}} = \left\{ \begin{array}{l} \left(DMI, \ 0.7e^{(0.8)\pi i}, 0.1e^{(0.2)\pi i} \right), \left(EM, \ 0.6e^{(0.6)\pi i}, 0.3e^{(0.3)\pi i} \right), \\ \left(CSW, \ 0.6e^{(0.4)\pi i}, 0.2e^{(0.4)\pi i} \right), \left(NNS, \ 0.5e^{(0.5)\pi i}, 0.3e^{(0.4)\pi i} \right), \\ \left(FCS, \ 0.5e^{(0.4)\pi i}, 0.2e^{(0.4)\pi i} \right), \left(MSS, \ 0.4e^{(0.5)\pi i}, 0.4e^{(0.2)\pi i} \right) \end{array} \right\}$$

$$
\mathfrak{j} = \left\{
\begin{array}{c}
\left(IS,\ 0.4e^{(0.5)\pi i}, 0.5e^{(0.5)\pi i}\right), \left(E\&DT,\ 0.5e^{(0.6)\pi i}, 0.5e^{(0.2)\pi i}\right), \\[4pt]
\left(ECM,\ 0.4e^{(0.4)\pi i}, 0.6e^{(0.5)\pi i}\right), \left(RW,\ 0.6e^{(0.7)\pi i}, 0.4e^{(0.2)\pi i}\right), \\[4pt]
\left(InT, 0.4e^{(0.3)\pi i}, 0.6e^{(0.6)\pi i}\right)
\end{array}
\right\}
$$

With the intention of determining the effectiveness of the security methods against each threat, we calculate the CP $\acute{I} \times \mathfrak{j}$. By using Definition 8, we have

$$
I \times \mathfrak{j} = \left\{
\begin{array}{c}
\left((DMI, IS), 0.4e^{(0.5)\pi i}, 0.5e^{(0.5)\pi i}\right), \left((DMI, E\&DT), 0.5e^{(0.6)\pi i}, 0.5e^{(0.2)\pi i}\right), \\[4pt]
\left((DMI, ECM), 0.4e^{(0.4)\pi i}, 0.2e^{(0.4)\pi i}\right), \left((DMI, RW), 0.6e^{(0.7)\pi i}, 0.4e^{(0.2)\pi i}\right), \\[4pt]
\left((DMI, InT), 0.4e^{(0.3)\pi i}, 0.6e^{(0.6)\pi i}\right), \left((EM, IS), 0.4e^{(0.5)\pi i}, 0.5e^{(0.5)\pi i}\right), \\[4pt]
\left((EM, E\&DT), 0.5e^{(0.6)\pi i}, 0.5e^{(0.3)\pi i}\right), \left((EM, ECM), 0.4e^{(0.4)\pi i}, 0.6e^{(0.5)\pi i}\right), \\[4pt]
\left((EM, RW), 0.6e^{(0.6)\pi i}, 0.4e^{(0.3)\pi i}\right), \left((EM, InT), 0.4e^{(0.3)\pi i}, 0.6e^{(0.6)\pi i}\right), \\[4pt]
\left((CSW, IS), 0.4e^{(0.4)\pi i}, 0.5e^{(0.5)\pi i}\right), \left((CSW, E\&DT), 0.5e^{(0.4)\pi i}, 0.5e^{(0.4)\pi i}\right), \\[4pt]
\left((CSW, ECM),\ 0.4e^{(0.4)\pi i}, 0.6e^{(0.5)\pi i}\right), \left((CSW, RW),\ 0.6e^{(0.4)\pi i}, 0.4e^{(0.4)\pi i}\right), \\[4pt]
\left((CSW, InT), 0.4e^{(0.3)\pi i}, 0.6e^{(0.6)\pi i}\right), \left((NNS, IS), 0.4e^{(0.5)\pi i}, 0.5e^{(0.5)\pi i}\right), \\[4pt]
\left((NNS, E\&DT),\ 0.5e^{(0.5)\pi i}, 0.5e^{(0.4)\pi i}\right), \left((NNS, ECM), 0.4e^{(0.4)\pi i}, 0.6e^{(0.5)\pi i}\right), \\[4pt]
\left((NNS, RW),\ 0.5e^{(0.5)\pi i}, 0.4e^{(0.4)\pi i}\right), \left((NNS, InT), 0.4e^{(0.3)\pi i}, 0.6e^{(0.6)\pi i}\right), \\[4pt]
\left((FCS, IS),\ 0.4e^{(0.4)\pi i}, 0.5e^{(0.5)\pi i}\right), \left((FCS, E\&DT), 0.5e^{(0.4)\pi i}, 0.5e^{(0.4)\pi i}\right), \\[4pt]
\left((FCS, ECM), 0.4e^{(0.4)\pi i}, 0.6e^{(0.5)\pi i}\right), \left((FCS, RW),\ 0.5e^{(0.4)\pi i},\ 0.4e^{(0.4)\pi i}\right), \\[4pt]
\left((FCS, InT), 0.4e^{(0.3)\pi i}, 0.6e^{(0.6)\pi i}\right), \left((MSS, IS), 0.4e^{(0.5)\pi i}, 0.5e^{(0.5)\pi i}\right), \\[4pt]
\left((MSS, E\&DT),\ 0.4e^{(0.5)\pi i}, 0.5e^{(0.2)\pi i}\right), \left((MSS, ECM), 0.4e^{(0.4)\pi i}, 0.6e^{(0.5)\pi i}\right), \\[4pt]
\left((MSS, RW),\ 0.4e^{(0.5)\pi i}, 0.4e^{(0.2)\pi i}\right), \left((MSS, InT), 0.4e^{(0.3)\pi i}, 0.6e^{(0.6)\pi i}\right)
\end{array}
\right\}
$$

Each element of $\acute{I} \times \mathfrak{j}$ is in the form of an order pair, which represents the relationship among the pair, i.e., the effects and impacts of the first term on the second term in the pair. The membership grades indicate the effectiveness of a security technique to eliminate a particular threat with respect to some time unit. On the other hand, the non-membership grades reflect the uselessness or ineffectiveness of a certain security method against a specific threat. For example, the element $\left((EM, RW), 0.6e^{(0.6)\pi i}, 0.4e^{(0.3)\pi i}\right)$ conveys that the event monitoring solution can effectively resolve the ransomware and the level of ineffectiveness is low. The numbers translate as follows: the level of security of event monitoring solution against the ransomware is 0.6 with respect to 0.6 time units and the level of risk due to ransomware after applying the event monitoring solution is 0.4 with respect to 0.3 time units. Regarding the security, a greater timeframe in the membership grade is better, while a shorter time in the non-membership grade is better. The diagrams in Figure 7 demonstrate the above relationships.

(**a**) Effects of *DMI* on each threat

(**b**) Effects of *EM* on each threat

(**c**) Effects of *CSW* on each threat

(**d**) Effects of *NNS* on each threat

(**e**) Effects of *FCS* on each threat

(**f**) Effects of *MSS* on each threat

**Figure 7.** Effects of different cyber-security measures on each threat.

5.2. Selection of the Cyber-Security Techniques

Suppose that an enterprise or company wishes to implement some cyber-security techniques in order to control and counter the potential threats and reduce the risks of cyber-attacks. There are certain possible techniques, which are given in the following Table 3. However, the company needs to select the best possible techniques that would resolve the issues that are being faced. The complete process of this application is shown in Figure 8.

Table 3. Abbreviations of cyber-security measures.

Cyber-Security	Abbreviation
Deep Armor Industrial	*DMI*
Event Monitoring	*EM*
Cyber-security workplace	*CSW*
Nozomi Network solution	*NNS*
Forge Cyber-Security Suite	*FCS*
Managed Security Services	*MSS*
Block Chain	*BC*
Firewall	*FW*
Security Softwares	*SSW*
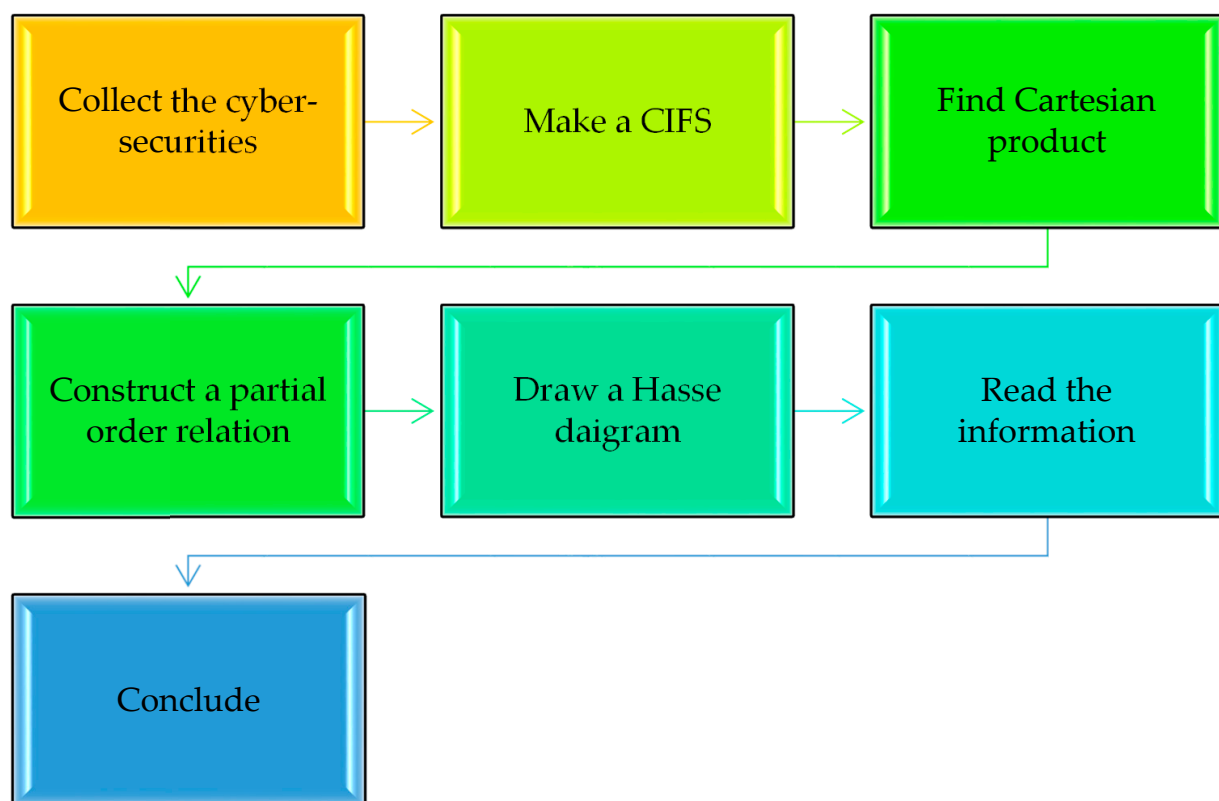
Figure 8. Flowchart of the process for selecting the best cyber-security measure.

Let us assign the supposed membership and non-membership grades to each of the security measures and construct a CIFS Í:

$$
Í = \left\{
\begin{array}{c}
\left(DMI,\ 0.7e^{(0.8)\pi i}, 0.1e^{(0.2)\pi i} \right), \left(EM,\ 0.6e^{(0.6)\pi i}, 0.3e^{(0.3)\pi i} \right), \\
\left(CSW,\ 0.6e^{(0.4)\pi i}, 0.2e^{(0.4)\pi i} \right), \left(NNS,\ 0.5e^{(0.5)\pi i}, 0.3e^{(0.4)\pi i} \right), \\
\left(FCS,\ 0.5e^{(0.4)\pi i}, 0.2e^{(0.4)\pi i} \right), \left(MSS,\ 0.4e^{(0.5)\pi i}, 0.4e^{(0.2)\pi i} \right), \\
\left(BC,\ 0.8e^{(0.8)\pi i}, 0.2e^{(0.1)\pi i} \right), \left(FW,\ 0.5e^{(0.6)\pi i}, 0.1e^{(0.2)\pi i} \right), \\
\left(SSW,\ 0.3e^{(0.4)\pi i}, 0.5e^{(0.6)\pi i} \right)
\end{array}
\right\}
$$

Based on the CP $Í \times Í$ (using Definition 8), a complex intuitionistic partial order FR *R* (Definition 9) is obtained:

$$
R = \left\{
\begin{array}{c}
\left((DMI, DMI), 0.7e^{(0.8)\pi i}, 0.1e^{(0.2)\pi i} \right), \left((DMI, BC), 0.7e^{(0.8)\pi i}, 0.2e^{(0.2)\pi i} \right), \\
\left((EM, EM), 0.6e^{(0.6)\pi i}, 0.3e^{(0.3)\pi i} \right), \left((EM, BC), 0.6e^{(0.6)\pi i}, 0.3e^{(0.3)\pi i} \right), \\
\left((CSW, EM), 0.6e^{(0.4)\pi i}, 0.3e^{(0.4)\pi i} \right), \left((CSW, CSW), 0.6e^{(0.4)\pi i}, 0.2e^{(0.4)\pi i} \right), \\
\left((CSW, BC), 0.6e^{(0.4)\pi i}, 0.2e^{(0.4)\pi i} \right), \left((NNS, DMI),\ 0.5e^{(0.5)\pi i}, 0.3e^{(0.4)\pi i} \right), \\
\left((NNS, EM),\ 0.5e^{(0.5)\pi i}, 0.3e^{(0.4)\pi i} \right), \left((NNS, NNS),\ 0.5e^{(0.5)\pi i}, 0.3e^{(0.4)\pi i} \right), \\
\left((NNS, BC),\ 0.5e^{(0.5)\pi i}, 0.3e^{(0.4)\pi i} \right), \left((FCS, DMI),\ 0.5e^{(0.4)\pi i}, 0.2e^{(0.4)\pi i} \right), \\
\left((FCS, EM),\ 0.5e^{(0.4)\pi i}, 0.3e^{(0.4)\pi i} \right), \left((FCS, NNS),\ 0.5e^{(0.4)\pi i}, 0.3e^{(0.4)\pi i} \right), \\
\left((FCS, FCS),\ 0.5e^{(0.4)\pi i}, 0.2e^{(0.4)\pi i} \right), \left((FCS, FW),\ 0.5e^{(0.4)\pi i}, 0.2e^{(0.4)\pi i} \right), \\
\left((FCS, BC),\ 0.5e^{(0.4)\pi i}, 0.2e^{(0.4)\pi i} \right), \left((MSS, EM), 0.4e^{(0.5)\pi i}, 0.4e^{(0.3)\pi i} \right), \\
\left((MSS, CSW), 0.4e^{(0.5)\pi i}, 0.4e^{(0.4)\pi i} \right), \left((MSS, MSS),\ 0.4e^{(0.5)\pi i}, 0.4e^{(0.2)\pi i} \right), \\
\left((MSS, BC),\ 0.4e^{(0.5)\pi i}, 0.4e^{(0.2)\pi i} \right), \left((BC, BC), 0.8e^{(0.8)\pi i}, 0.2e^{(0.1)\pi i} \right), \\
\left((FW, DMI), 0.5e^{(0.6)\pi i}, 0.1e^{(0.2)\pi i} \right), \left((FW, EM), 0.5e^{(0.6)\pi i}, 0.3e^{(0.3)\pi i} \right), \\
\left((FW, NNS), 0.5e^{(0.5)\pi i}, 0.3e^{(0.4)\pi i} \right), \left((FW, FW), 0.5e^{(0.6)\pi i}, 0.1e^{(0.2)\pi i} \right), \\
\left((FW, BC), 0.5e^{(0.6)\pi i}, 0.2e^{(0.2)\pi i} \right), \left((SSW, DMI), 0.3e^{(0.4)\pi i}, 0.5e^{(0.6)\pi i} \right), \\
\left((SSW, EM), 0.3e^{(0.4)\pi i}, 0.5e^{(0.6)\pi i} \right), \left((SSW, CSW), 0.3e^{(0.4)\pi i}, 0.5e^{(0.6)\pi i} \right), \\
\left((SSW, NNS) 0.3e^{(0.4)\pi i}, 0.5e^{(0.6)\pi i} \right), \left((SSW, FCS), 0.3e^{(0.4)\pi i}, 0.5e^{(0.6)\pi i} \right), \\
\left((SSW, MSS), 0.3e^{(0.4)\pi i}, 0.5e^{(0.6)\pi i} \right), \left((SSW, BC), 0.3e^{(0.4)\pi i}, 0.5e^{(0.6)\pi i} \right), \\
\left((SSW, FW), 0.3e^{(0.4)\pi i}, 0.5e^{(0.6)\pi i} \right), \left((SSW, SSW),\ 0.3e^{(0.4)\pi i}, 0.5e^{(0.6)\pi i} \right)
\end{array}
\right\}
$$

Using the Definition 13, the Hasse diagram for the above complex intuitionistic partial order FR is constructed, which is given in Figure 9. For convenience, the membership and non-membership grades are not listed in the diagram. According to *R*, block chain is the best security technique among the available competitors because it is the maximum as well as the maximal element (according to Definition 14), while security software such as antivirus and antimalware software provides the least security because *SSW* is the minimum as well as the minimal element of the diagram (according to Definition 14).

Assume that the company has certain priorities, and the following security techniques have been separated from a larger set of techniques. These security measures are listed in the subset ȷ, which is indicated in blue in the diagram.

$$
ȷ = \left\{
\begin{array}{c}
\left(NNS,\ 0.5e^{(0.5)\pi i}, 0.3e^{(0.4)\pi i} \right), \left(FCS,\ 0.5e^{(0.4)\pi i}, 0.2e^{(0.4)\pi i} \right), \\
\left(FW,\ 0.5e^{(0.6)\pi i}, 0.1e^{(0.2)\pi i} \right), \left(SSW,\ 0.3e^{(0.4)\pi i}, 0.5e^{(0.6)\pi i} \right)
\end{array}
\right\}
$$

The objective is to choose the best security technique among the members of set ȷ. Thus, one may be interested in the upper bounds and supremum. In this case, according to Definition 15, the upper bounds are $\{DMI, EM, NNS, BC\}$. By Definition 16, the supremum is the lowest upper bound, which is NNS. Hence, the Nozomi network solution is the most suitable cyber-security measure among the shortlisted ones that will eliminate the threats or reduce the risks of cyber-attacks.
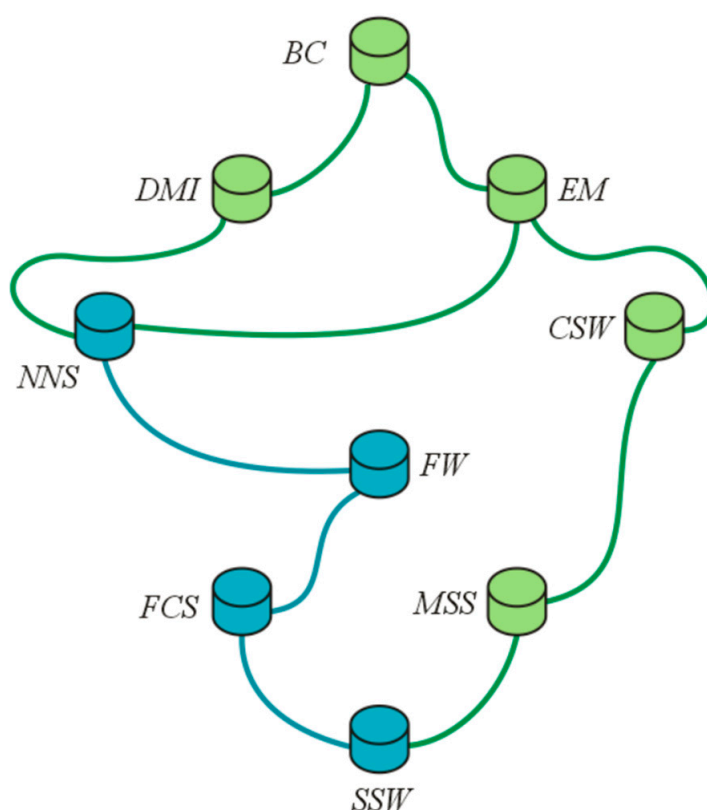
.

Figure 9. Hasse diagram for *FR*.

6. Comparative Analysis

In this section, the omnipotence of the proposed framework of CIFRs is verified through a comparison of CIFRs with the existing structures such as CFRs or IFRs.

The major advantage of a CIFR over FR and IFR is the complex-valued membership and non-membership grades. The structure of a CIFR is composed of amplitude term and phase term, which enable it to model the situations with phase alteration and periodicity. On the other hand, the FRs and IFRs lack the phase term; thus, they are limited to only single dimensional models.

Meanwhile, the structure of CFRs is based on a complex number and thus consists of amplitude and phase terms. A detailed comparison between CIFRs and other structures is given in the following subsections.

6.1. CIFRs vs. CFRs

Let us study the relationships between the set of cyber-security techniques and cyber-crimes using the CFRs. As CFRs are superior to FRs, the comparison is carried out between CIFRs and CFRs. Consider the following two CFSs Í and ȷ representing the set of security

measures and the set of threats, respectively. The details of the abbreviations used in sets Í and j are given in Tables 4 and 5.

$$\acute{I} = \left\{ \begin{array}{l} \left(DMI,\ 0.7e^{(0.8)\pi i} \right), \left(EM,\ 0.6e^{(0.6)\pi i} \right), \left(CSW,\ 0.6e^{(0.4)\pi i} \right), \\ \left(NNS,\ 0.5e^{(0.5)\pi i} \right), \left(FCS,\ 0.5e^{(0.4)\pi i} \right), \left(MSS,\ 0.4e^{(0.5)\pi i} \right) \end{array} \right\}$$

$$j = \left\{ \begin{array}{l} \left(IS,\ 0.4e^{(0.5)\pi i} \right), \left(E\&DT,\ 0.5e^{(0.6)\pi i} \right), \left(ECM,\ 0.4e^{(0.4)\pi i} \right), \\ \left(RW,\ 0.6e^{(0.7)\pi i} \right), \left(InT, 0.4e^{(0.3)\pi i} \right) \end{array} \right\}$$

Table 4. Abbreviations of security measures in set j.

Security Method	Abbreviation
Deep Armor Industrial	DMI
Event Monitoring	EM
Cyber-security workplace	CSW
Nozomi Network solution	NNS
Forge Cyber-Security Suite	FCS
Managed Security Services	MSS

Table 5. Abbreviations of threats in set j.

Threat	Abbreviation
Infrastructure sabotage	IS
Espionage and data theft	E&DT
Ever-changing malware	ECM
Ransomware	RW
Insider threat	InT

By applying the procedure detailed in Figure 6, the following CFR *R* is found, which discusses the effectiveness of security methods against each threat:

$$R = \left\{ \begin{array}{l} \left((DMI, IS), 0.4e^{(0.5)\pi i} \right), \left((DMI, E\&DT), 0.5e^{(0.6)\pi i} \right), \left((DMI, ECM), 0.4e^{(0.4)\pi i} \right), \\ \left((DMI, RW), 0.6e^{(0.7)\pi i} \right), \left((DMI, InT), 0.4e^{(0.3)\pi i} \right), \left((EM, IS), 0.4e^{(0.5)\pi i} \right), \\ \left((EM, E\&DT), 0.5e^{(0.6)\pi i} \right), \left((EM, ECM), 0.4e^{(0.4)\pi i} \right), \left((EM, RW), 0.6e^{(0.6)\pi i} \right), \\ \left((EM, InT), 0.4e^{(0.3)\pi i} \right), \left((CSW, IS), 0.4e^{(0.4)\pi i} \right), \left((CSW, E\&DT), 0.5e^{(0.4)\pi i} \right), \\ \left((CSW, ECM),\ 0.4e^{(0.4)\pi i} \right), \left((CSW, RW),\ 0.6e^{(0.4)\pi i} \right), \left((CSW, InT), 0.4e^{(0.3)\pi i} \right), \\ \left((NNS, IS), 0.4e^{(0.5)\pi i} \right), \left((NNS, E\&DT),\ 0.5e^{(0.5)\pi i} \right), \left((NNS, ECM), 0.4e^{(0.4)\pi i} \right), \\ \left((NNS, RW),\ 0.5e^{(0.5)\pi i} \right), \left((NNS, InT), 0.4e^{(0.3)\pi i} \right), \left((FCS, IS),\ 0.4e^{(0.4)\pi i} \right), \\ \left((FCS, E\&DT), 0.5e^{(0.4)\pi i} \right), \left((FCS, ECM), 0.4e^{(0.4)\pi i} \right), \left((FCS, RW),\ 0.5e^{(0.4)\pi i} \right), \\ \left((FCS, InT), 0.4e^{(0.3)\pi i} \right), \left((MSS, IS), 0.4e^{(0.5)\pi i} \right), \left((MSS, E\&DT),\ 0.4e^{(0.5)\pi i} \right), \\ \left((MSS, ECM), 0.4e^{(0.4)\pi i} \right), \left((MSS, RW),\ 0.4e^{(0.5)\pi i} \right), \left((MSS, InT), 0.4e^{(0.3)\pi i} \right) \end{array} \right\}$$

Each of the elements in the above CFR demonstrates the connection between a pair of elements in an ordered pair. The effects of the first element (appearing first in the ordered pair) on the second element (appearing latter in the ordered pair) are described by the membership grades. Since the Cartesian product is carried out from the set of security measures to the set of threats, the found relation indicates the effects of the security measures on the threats. Since it is a CFR, its membership grades only display the effectiveness of a cyber-security measure against a particular threat. It also fails to provide

valuable information about the ineffectiveness and failure levels of each cyber-security measure against certain threats. Meanwhile, the CIFRs provide the complete information. Hence, this shows the dominance of CIFRs over CFRs and FRs.

6.2. CIFRs vs. IFRs

In this section, the IFRs and IFSs are used to investigate the matter discussed in the proposed applications, i.e., the relationships between the set of cyber-security techniques and the set of cyber-crimes. Consider the following two IFSs $Í$ and $ȷ$ representing the set of security measures and the set of threats, respectively. The details of the abbreviations used in sets $Í$ and $ȷ$ are given in Tables 4 and 5.

$$Í = \left\{ \begin{array}{c} (DMI,\ 0.7, 0.1), (EM,\ 0.6, 0.3), (CSW,\ 0.6, 0.2), \\ (NNS,\ 0.5, 0.3), (FCS,\ 0.5, 0.2), (MSS,\ 0.4, 0.4) \end{array} \right\}$$

$$ȷ = \left\{ \begin{array}{c} (IS,\ 0.4, 0.5), (E\&DT,\ 0.5, 0.5), (ECM,\ 0.4, 0.6), \\ (RW,\ 0.6, 0.4), (InT, 0.4, 0.6) \end{array} \right\}$$

Following the process discussed in Figure 6, the following IFR R is obtained, which discusses the usefulness of the security methods against each threat:

$$R = \left\{ \begin{array}{c} ((DMI, IS), 0.4, 0.5), ((DMI, E\&DT), 0.5, 0.5), ((DMI, ECM), 0.4, 0.2), \\ ((DMI, RW), 0.6, 0.4), ((DMI, InT), 0.4, 0.6), ((EM, IS), 0.4, 0.5), \\ ((EM, E\&DT), 0.5, 0.5), ((EM, ECM), 0.4, 0.6), ((EM, RW), 0.6, 0.4), \\ ((EM, InT), 0.4, 0.6), ((CSW, IS), 0.4, 0.5), ((CSW, E\&DT), 0.5, 0.5), \\ ((CSW, ECM),\ 0.4, 0.6), ((CSW, RW),\ 0.6, 0.4), ((CSW, InT), 0.4, 0.6), \\ ((NNS, IS), 0.4, 0.5), ((NNS, E\&DT),\ 0.5, 0.5), ((NNS, ECM), 0.4, 0.6), \\ ((NNS, RW),\ 0.5, 0.4), ((NNS, InT), 0.4, 0.6), ((FCS, IS),\ 0.4, 0.5), \\ ((FCS, E\&DT), 0.5, 0.5), ((FCS, ECM), 0.4, 0.6), ((FCS, RW),\ 0.5,\ 0.4), \\ ((FCS, InT), 0.4, 0.6), ((MSS, IS), 0.4, 0.5), ((MSS, E\&DT),\ 0.4, 0.5), \\ ((MSS, ECM), 0.4, 0.6), ((MSS, RW),\ 0.4, 0.4), ((MSS, InT), 0.4, 0.6) \end{array} \right\}$$

Based on the information in the above IFR, each element shows the relationship between a pair of elements. The approach to the interpretation of the information and determination of the results is similar to the previous examples. Thus, being an IFR, it only contains the amplitude terms, and the phase terms are missing. It produces incomplete results because the duration is missing. Therefore, it only defines the effectiveness and ineffectiveness of the cyber-security measures against the threats through the membership grade and non-membership grade, respectively. This structure is unsuccessful in providing the required results. The CIFRs produce satisfactory results that are required to obtain detailed information. Hence, this example illustrates the supremacy of CIFRs over IFRs. For this reason, this article chose the structure of CIFR to analyze the matter of cyber-security and cyber-crimes in the oil and gas industries.

7. Conclusions

This article introduces the novel concepts of complex intuitionistic fuzzy relation (CIFR) and the Cartesian product of two complex intuitionistic fuzzy sets (CIFSs). In addition, the types of CIFRs are defined, such as equivalence, pre-order, partial order, total order, strict order relations, equivalence class and the composition of two CIFRs. Moreover, the Hasse diagram of complex intuitionistic partial order fuzzy relations is introduced. The notions of maximum, minimum, maximal, minimal, supremum and infimum, etc., are defined for a Hasse diagram. The development of these innovative frameworks and novel modeling techniques aims to address the cyber-security concerns in the oil and gas industries. These industries have recently been targeted by hackers and cyber-criminals. Thus, the current study analyzes the relationships among the effectiveness of cyber-security

measures and the most serious and common risks to the mentioned industries. Then, the CIFRs are applied for the security analysis of the oil and gas industries to explore the effects of certain cyber-security measures on the threats. Moreover, the complex intuitionistic partial order fuzzy relation and the Hasse diagram are used to determine the most appropriate cyber-security method for an industry. Lastly, the proposed methods are compared with the other methods in the literature. The weaknesses of the proposed methods include the absence of a neutral grade as well as the limitations and the constraints on the sum of grades. In future, these concepts can be extended to the other generalizations of fuzzy sets [48–51], which will give rise to many interesting structures with a vast range of applications.

References

1. Klir, G.J.; Folger, T.A. *Fuzzy Sets, Uncertainty, and Information*; Englewood Cliffs, Prentice Hall: Hoboken, NJ, USA, 1988.
2. Zadeh, L.A. Fuzzy sets. *Inf. Control.* **1965**, *8*, 338–353. [CrossRef]
3. Mendel, J.M. Fuzzy logic systems for engineering: A tutorial. *Proc. IEEE* **1995**, *83*, 345–377. [CrossRef]
4. Torra, V. Hesitant fuzzy sets. *Int. J. Intell. Syst.* **2010**, *25*, 529–539. [CrossRef]
5. Zadeh, L.A. Fuzzy sets as a basis for a theory of possibility. *Fuzzy Sets Syst.* **1978**, *1*, 3–28. [CrossRef]
6. Negoiţă, C.V.; Ralescu, D.A. *Applications of Fuzzy Sets to System Analysis*; Birkhäuser: Basel, Switzerland, 1975; p. 187.
7. Goguen, J.A. L-fuzzy sets. *J. Math Anal. Apps.* **1967**, *18*, 145–174. [CrossRef]
8. Laengle, S.; Lobos, V.; Merigó, J.M.; Herrera-Viedma, E.; Cobo, M.J.; De Baets, B. Forty years of fuzzy sets and systems: A bibliometric analysis. *Fuzzy Sets Syst.* **2021**, *402*, 155–183. [CrossRef]
9. Xu, W.J.; He, L.J.; Zhu, G.Y. Many-objective flow shop scheduling optimisation with genetic algorithm based on fuzzy sets. *Int. J. Prod. Res.* **2021**, *59*, 702–726. [CrossRef]
10. Mewada, S.; Sharma, P.; Gautam, S.S. Exploration of fuzzy system with applications. In *Research Anthology on Multi-Industry Uses Genetic Programming and Algorithms*; IGI Global: Hershey, PA, USA, 2021; pp. 550–569.
11. Ramot, D.; Milo, R.; Friedman, M.; Kandel, A. Complex fuzzy sets. *IEEE Trans. Fuzzy Syst.* **2002**, *10*, 171–186. [CrossRef]
12. Ramot, D.; Friedman, M.; Langholz, G.; Kandel, A. Complex fuzzy logic. *IEEE Trans. Fuzzy Syst.* **2003**, *11*, 450–461. [CrossRef]
13. Pedrycz, W. Fuzzy Relations and Relational Computing. In *Introduction to Computing with Fuzzy Sets*; Springer: Cham, Switzerland, 2021; pp. 49–65.
14. Yu, D.; Hu, Q.; Wu, C. Uncertainty measures for fuzzy relations and their applications. *Appl. Soft Comput.* **2007**, *7*, 1135–1143. [CrossRef]
15. De Baets, B.; Kerre, E. Fuzzy relations and applications. In *Advances in Electronics and Electron. Physics*; Academic Press: Cambridge, MA, USA, 1994; Volume 89, pp. 255–324.
16. Tamura, S.; Higuchi, S.; Tanaka, K. Pattern classification based on fuzzy relations. *IEEE Trans. Syst. Man Cybern.* **1971**, *1*, 61–66. [CrossRef]
17. Bhattacharya, P.; Mukherjee, N.P. Fuzzy relations and fuzzy groups. *Inf. Sci.* **1985**, *36*, 267–282. [CrossRef]
18. Braae, M.; Rutherford, D.A. Fuzzy relations in a control setting. *Kybernetes* **1978**, *7*, 185–188. [CrossRef]

19. Zhang, G.; Dillon, T.S.; Cai, K.Y.; Ma, J.; Lu, J. Operation properties and δ-equalities of complex fuzzy sets. *Int. J. Approx. Reason.* **2009**, *50*, 1227–1249. [CrossRef]
20. Yazdanbakhsh, O.; Dick, S. A systematic review of complex fuzzy sets and logic. *Fuzzy Sets Syst.* **2018**, *338*, 1–22. [CrossRef]
21. Tamir, D.E.; Rishe, N.D.; Kandel, A. Complex fuzzy sets and complex fuzzy logic an overview of theory and applications. *Fifty Years Fuzzy Log. Its Appl.* **2015**, 661–681. [CrossRef]
22. Ma, J.; Zhang, G.; Lu, J. A method for multiple periodic factor prediction problems using complex fuzzy sets. *IEEE Trans. Fuzzy Syst.* **2011**, *20*, 32–45.
23. Nasir, A.; Jan, N.; Gumaei, A.; Khan, S.U. Medical diagnosis and life span of sufferer using interval valued complex fuzzy relations. *IEEE Access* **2021**, *9*, 93764–93780. [CrossRef]
24. Atanassov, K.T. Intuitionistic fuzzy sets. *Fuzzy Sets Syst.* **1986**, *20*, 87–96. [CrossRef]
25. Burillo, P.; Bustince, H. Intuitionistic fuzzy relations (Part I). *Math Soft Comput.* **1995**, *2*, 5–38.
26. De, S.K.; Biswas, R.; Roy, A.R. An application of intuitionistic fuzzy sets in medical diagnosis. *Fuzzy Sets Syst.* **2001**, *117*, 209–213. [CrossRef]
27. Szmidt, E.; Kacprzyk, J. Distances between intuitionistic fuzzy sets. *Fuzzy Sets Syst.* **2000**, *114*, 505–518. [CrossRef]
28. De, S.K.; Biswas, R.; Roy, A.R. Some operations on intuitionistic fuzzy sets. *Fuzzy Sets Syst.* **2000**, *114*, 477–484. [CrossRef]
29. Gerstenkorn, T.; Mańko, J. Correlation of intuitionistic fuzzy sets. *Fuzzy Sets Syst.* **1991**, *44*, 39–43. [CrossRef]
30. Büyüközkan, G.; Uztürk, D. Smart Fridge Design with Interval-Valued Intuitionistic Fuzzy QFD. In *International Conference Intelligent & Fuzzy Systems*; Springer: Cham, Switzerland, 2019; pp. 1170–1179.
31. Rani, D.; Garg, H. Complex intuitionistic fuzzy preference relations and their applications in individual and group decision-making problems. *Int. J. Intell. Syst.* **2021**, *36*, 1800–1830. [CrossRef]
32. Bustince, H.; Burillo, P. Structures on intuitionistic fuzzy relations. *Fuzzy Sets Syst.* **1996**, *78*, 293–303. [CrossRef]
33. Deschrijver, G.; Kerre, E.E. On the composition of intuitionistic fuzzy relations. *Fuzzy Sets Syst.* **2003**, *136*, 333–361. [CrossRef]
34. Alkouri, A.S.; Salleh, A.R. Complex intuitionistic fuzzy sets. *AIP Conf. Proc.* **2012**, *1482*, 464.
35. Yaqoob, N.; Gulistan, M.; Kadry, S.; Wahab, H.A. Complex intuitionistic fuzzy graphs with application in cellular network provider companies. *Math* **2019**, *7*, 35. [CrossRef]
36. Nasir, A.; Jan, N.; Yang, M.-S.; Khan, S.U. Complex T-spherical fuzzy relations with their applications in economic relationships and international trades. *IEEE Access* **2021**, *9*, 66115–66131. [CrossRef]
37. Nasir, A.; Jan, N.; Gumaei, A.; Khan, S.U.; Al-Rakhami, M. Evaluation of the Economic Relationships on the Basis of Statistical Decision-Making in Complex Neutrosophic Environment. *Complexity* **2021**, *2021*, 5595474. [CrossRef]
38. Ngan, R.T.; Ali, M.; Tamir, D.E.; Rishe, N.D.; Kandel, A. Representing complex intuitionistic fuzzy set by quaternion numbers and applications to decision making. *Appl. Soft Comput.* **2020**, *87*, 105961. [CrossRef]
39. Kumar, T.; Bajaj, R.K. On complex intuitionistic fuzzy soft sets with distance measures and entropies. *J. Math.* **2014**, *2014*, 972198. [CrossRef]
40. Lamba, A. Protecting 'Cybersecurity & Resiliency'of Nation's Critical Infrastructure—Energy, Oil & Gas. *Int. J. Curr. Res.* **2018**, *10*, 76865–76876.
41. Line, M.B.; Tøndel, I.A.; Jaatun, M.G. Cyber security challenges in Smart Grids. In Proceedings of the 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies, Manchester, UK, 5–7 December 2011; pp. 1–8.
42. Lu, H.; Huang, K.; Azimi, M.; Guo, L. Blockchain technology in the oil and gas industry: A review of applications, opportunities, challenges, and risks. *IEEE Access* **2019**, *7*, 41426–41444. [CrossRef]
43. Lakhanpal, V.; Samuel, R. Implementing blockchain technology in oil and gas industry: A review. One Petro. In Proceedings of the SPE Annual Technical Conference and Exhibition, Dallas, TX, USA, 24–26 September 2018. [CrossRef]
44. Yang, L.; Cao, X.; Li, J. A new cyber security risk evaluation method for oil and gas SCADA based on factor state space. *Chaos Solitons Fractals* **2016**, *89*, 203–209. [CrossRef]
45. Stergiopoulos, G.; Gritzalis, D.A.; Limnaios, E. Cyber-attacks on the Oil & Gas sector: A survey on incident assessment and attack patterns. *IEEE Access* **2020**, *8*, 128440–128475.
46. Wanasinghe, T.R.; Gosine, R.G.; James, L.A.; Mann, G.K.; De Silva, O.; Warrian, P.J. The Internet of things in the oil and gas industry: A systematic review. *IEEE Internet Things J.* **2020**, *7*, 8654–8673. [CrossRef]
47. Bjerga, T.; Aven, T. Adaptive risk management using new risk perspectives–an example from the oil and gas industry. *Reliab. Eng. Syst. Saf.* **2015**, *134*, 75–82. [CrossRef]
48. Ali, Z.; Mahmood, T.; Ullah, K.; Khan, Q. Einstein Geometric Aggregation Operators Using a Novel Complex Interval-Valued Pythagorean Fuzzy Setting with Application in Green Supplier Chain Management. *Rep. Mech. Eng.* **2021**, *2*, 105–134. [CrossRef]
49. Riaz, M.; Çagman, N.; Wali, N.; Mushtaq, A. Certain Properties of Soft Multi-Set Topology with Applications in Multi-Criteria Decision Making. *Decis. Mak. Appl. Manag. Eng.* **2020**, *3*, 70–96. [CrossRef]
50. Bozanic, D.; Milic, A.; Tesic, D.; Salabun, W.; Pamucar, D. D numbers-FUCOM-Fuzzy RAFSI model for selecting the group of construction machines for enabling mobility. *Facta Univ. Ser. Mech. Eng.* **2021**, *19*, 1–23. [CrossRef]
51. Ramakrishnan, K.R.; Chakraborty, S. A cloud TOPSIS model for green supplier selection. *Facta Univ. Ser. Eng.* **2020**, *18*, 375–397.