Sustainable Machine Intelligence Journal

Journal Homepage: sciencesforce.com/smij

Sustain. Mach. Intell. J. Vol. 9 (2024) 89–101

Paper Type: Original Article

# Innovative Soft Cryptosystem for Encrypting and Decrypting Messages with IDEA

**Muhammad Saeed** [1,*], **Hafiz Inam ul Haq** [1], **Mubashir Ali** [1] **and Mudassira Mustafa** [1]

[1] Department of Mathematics, University of Management and Technology Lahore, 54770, Pakistan;
Emails: muhammad.saeed@umt.edu.pk; f2021109017@umt.edu.pk; v31553@umt.edu.pk; s2023109004@umt.edu.pk.

**Received:** 09 May 2024 **Revised:** 24 Aug 2024 **Accepted:** 27 Sep 2024 **Published:** 01 Oct 2024

## Abstract

This paper introduces an advanced cryptosystem for message encryption and decryption, integrating the International Data Encryption Algorithm (IDEA) with soft set and soft matrix principles. Soft sets, conceptualized by Molodtsov, are adept at managing uncertainty, making them ideal for cryptographic frameworks. Our approach utilizes inverse and characteristic products of soft sets and matrices, combined with the robust IDEA algorithm, to significantly enhance security. The IDEA algorithm operates on 64 -bit data blocks with a 128 -bit key, ensuring strong encryption. Additionally, we incorporate the symmetric to introduce complex permutations, further strengthening the cryptographic process by ensuring unique encryptions for identical plaintexts. This layered approach drastically improves resilience against unauthorized decryption. Practical applications demonstrate the system's efficacy, highlighting its superior security and reliability for data transmission in environments with high uncertainty. This innovative cryptosystem provides a formidable solution for contemporary encryption challenges.

**Keywords:** Soft Set; Soft Matrix; International Data Encryption Algorithm; IDEA Algorithm; Inverse and Characteristic Product.

## 1 | Introduction

In a time where technology progresses rapidly, the safety of sensitive information has turned out to be an urgent problem for individuals, organizations, and governments alike. The explosive rise of digital communication and the internet has made data exchange commonplace, thus it is one more pressing reason to protect information from unauthorized access or cyber threats. So, that is the kind of data that we have to handle under fuzziness, vagueness, and uncertainty conditions [1–2]. Security Encryption and Decryption: Original verification for data details. International Data Encryption Algorithm (IDEA) is a sound and secure encryption algorithm used to encrypt/decrypt messages. This is the introduction that describes in-depth encryption and decryption, how the IDEA algorithm works, implementation of fuzzy logic concepts[3] into a traditional cryptographic approach through soft cryptosystems. A pure soft set- an infinite mathematical structure is a new mathematical tool based on uncertainty and vagueness concepts to model the information in arbitrary forms using our routine implementation [4]. Unlike classical mathematical models, which frequently encounter ambiguities and a lack of data received from sensors etc. Pure soft sets are resistant to these corresponding complexities [2]. It tracks the way we are encrypted to decrypt or none with our

Corresponding Author: muhammad.saeed@umt.edu.pk

https://doi.org/10.61356/SMIJ.2024.9385

experience in digital signatures used for encryption and decryption. Soft set-based cryptosystems are considered an efficient approach that can deal with changeable conditions and ambiguity that may come while encrypting a message. This is very important in evolving new kinds of cryptographic techniques that are more robust, where the parameters and conditions for encryption can be created on the fly using soft set representations. Therefore, such verifiably universal PKE with a forbidden ciphertext space guarantees that the cryptosystem with stands all admissible attacks and works securely/efficiently in wide scenarios. To prevent unwanted access being prevented, the plaintext is instead translated into the unreadable format by the intended use of encryption and decryption [5]. Decryption, on the other hand, takes back your ciphertext to plain text for authorized users can read it. These processes are crucial to preempt any possible security breaches or cyberattacks on confidential information, like bank details, personal messages, and intimate data. This is where we used data such as bank records, private conversations, for high sensitivity and complexity to analyze this data [6]. Encryption ensures the integrity of confidentiality when intercepted by making it impossible to understand without a decryption key. Encryption is commercially used in metal, fast food containers, and IT companies to store data like e-commerce and online banking secure email facilities [7]. As new types of cyber threats [8] are emerging, the necessary for strong encryption methods does improve. To stay ahead of attackers who attacked encryption mathematically, cryptographic methods are constantly evolving and being improved [9].

Overview of IDEA algorithm (International Data Encryption Standard) Xuejia Lai and James L. Massey developed the IDEA in 1991 [10]. However, designed in 1993 to replace the older Data Encryption Standard (DES), increased its primary reason from DES key length of using other improved elements expected at that date any time possible for criminals reach demanding cryptanalysis. IDEA has a pad size of 128 with extra transformations that are hard to decrypt, thus providing a more reliable encryption algorithm [11]. IDEA uses symmetric key encryption, dealing with 64-bit data blocks [12]. It simplifies key management in that you use the same key for both encryption and decryption. This is the overall structure of the algorithm with 8 consecutive rounds and then after an output transformation round. These nonlinearity and diffusion operations are combined using three types of modular addition, multiplication, and bitwise XOR in each cycle to form the round functions which is a basic feature for strong encryption. One of the most appealing features of IDEA is that it has a built-in resistance to two very powerful methods used for deciphering cryptographic algorithms linear and differential cryptanalysis. The avalanche effect is just a result of how the algorithm and its ciphertexts are structured, ensuring that even small changes to plaintext or key will lead to vastly different-looking cipher cards. It then becomes very hard for attackers to guess or predict the key from the ciphertexts they have observed. The second paragraph is about Soft Cryptosystems even if traditional cryptographic algorithms such as those based on the IDEA (International Data Encryption Algorithm) have proven to be secure, we need new innovative techniques always because of exponentially growing fast cryptography attacks, the nature of cyber threats. Soft cryptosystems fuse the foundations of traditional cryptography with fuzzy logic, offering a new twist on security enabled through cryptographic means. Fuzzy logic, introduced by Zadeh [13] in 1965 is a way of solving fuzzy reasoning instead of the classic crisp and precise reasoning. Especially when dealing with real-world scenarios where information is often ambiguous or somewhat inaccurate, this method comes in handy. Soft cryptosystems use fuzzy logic in cryptography to increase the intricacy and adaptability of usual encryption schemes. Similarly, fuzzy logic-based cryptographic systems can act as per the risk factor or uncertainty attached to material being encrypted. This flexibility improves the security of encryption and resistance to attacks from malware like ransomware.

There are many advantages of these soft cryptosystems as compared to traditional cryptographic techniques [14]. For starters, they increase security by inserting fuzziness into the encryption process making it difficult for attackers to predict or model how a system will behave. Second, the adaptability of an ideal adversary provides a capacity to adjust for variations in threat level and security requirements counter-response to new threats if they arise. Soft cryptosystems could eventually reduce computation overhead with specialization over encryption settings to adapt to given needs and circumstances. Linked Soft Cryptosystems and IDEA significant breakthrough in the field of cryptography is the incorporation of the IDEA [15] into a soft cryptosystem approach. The proposed novel approach aims to merge the flexibility and robustness provided by fuzzy logic with the security attributes of IDEA, a well-known cryptosystem known as a "soft cryptosystem," the final product promises better message encryption, offering protections to ensure sensitive information remains secure against cyber threats. Some important steps of soft cryptosystem following this the concepts and workings of the IDEA algorithm were introduced which must be learnt & used in functioning beforehand. This framework is further elaborated using concepts from fuzzy logic [16] to allow the system settings in these IDEA processes to change adaptive regarding risk or uncertainty associated with given input. Decision matrix Zulqrnain and Saeed Fuzzy soft [17] to implement this type of integration there are a variety of methods, fuzzy inference systems which select appropriate encryption parameters for a given set of rules. The performance and security of the generated soft cryptosystem must be evaluated thoroughly. This includes testing the ability of the system to resist different types of attacks (differential and linear cryptanalysis [18]) on one hand, as well as its capability to handle various levels of data uncertainty. Furthermore, to guarantee the deployment of this system in real-world scenarios (i.e. outside a controlled environment), it is investigated if the proposed solution scale and be computed at realistic levels.

## 1.1| Study Objective and Scope

This paper examines a soft cryptosystem framework and gives an algorithm to encrypt and decrypt idea secret/key messages. The main motive of this research is to verify the efficiency and security gains obtained by combining fuzzy logic with traditional cryptography techniques. This study will include analyzing the algorithm, you need some basics and how this IDEA works as well as certain security features of that design and implementation of a soft cryptosystem proposal for a model that integrates the IDEA algorithm with fuzzy logic to create a soft cryptosystem. Second, assessing performance and security compared to the conventional IDEA implementation (IDEAlight), evaluating performance metrics of recommended soft cryptosystem and its security improvements. Real-world applications for the soft cryptosystem that demonstrate encryption and decryption of sensitive communications across various industries such as finance, healthcare, and communication.

## 1.2|Literature Review

In recent years, the area of cryptography [19] has significantly advanced due to a need to protect confidential information in an online world. This literature review emphasizes the concept used in IDEA [20] and a new soft cryptosystem that incorporates fuzzy logic principles, further sections explain major improvements have been made in an approach of encrypting as well as decrypting [21]. Let us study the work that has already been done and much more recent developments made in these fields to understand its pros/cons/potential directions of improvements for cryptographic security. A brief history of Cryptographic Algorithm Evolution the evolution from basic ciphers to encrypt communication is as old as the discovery of the cryptographic technique itself. This changed in the mid-1900s as computers came into use and more elaborate algorithms were developed, triggering a revolution in the field. The Data Encryption Standard (DES) was one of the first cryptographic algorithms to be widely adopted and used in the late 1970s. This was due to the early success DES had experienced and also that its key length is relatively short, therefore allowing brute-force attacks on its keys thus igniting the hunt for more secure alternatives.

Soft cryptosystems are an advanced concept in which the fuzzy logic ideas with conventional cryptography of pattern encryption methods, as been merged. Fuzzy Logic was introduced by Lotfi Zadeh in 1965 [26] and it's an approximate reasoning rather than the exact value of classical logic. This is why it can be particularly useful to handle uncertainty, fuzziness, or real-world situations since they contain ambiguity and imprecision. Using fuzzy logic in a cryptographic application will make the encryption methods more adaptable and resistant. Such a cryptosystem is considered to be soft as it adjusts the encryption parameters depending on how much unknown or dangerous level of data we are dealing with and therefore represents an even more flexible yet secure solution. Researchers showed fuzzy logic in Liu et al. [27] to be an efficient way of providing cryptographic systems with resistance against different types of attacks. Applications of and advantages in fuzzy logic for cryptography field applications advantages several fields have been using fuzzy logic to deal with imprecise, incomplete, or uncertain datasets. It holds the promise of enhancing the security and flexibility of encryption schemes in cryptography. For example, fuzzy logic can be employed to calculate the encryption strength based on the danger level perceived and material sensitivity. It is this flexibility that helps to ensure a secure and reliable method of encryption. One study on the use of fuzzy logic in key management and distribution, as conducted by Kumar and Tripathi [28], has presented how it can simplify these functions while reducing the risk of a bug compromise. Fuzzy logic can be used to create harder to measure and, thus more complex encryption techniques as well. Bringing soft cryptosystems and IDEA together unlocking the benefits of both paradigms is mandatory if one expects to amalgamate any soft cryptosystem with IDEA. IDEA's proven security and sound architecture make a solid underpinning, then fuzzy logic introduces an adaptable layer of complexity. This integration is designed to create a cryptography system that can adjust against new threats while still being secure. Patel et al. [29] have studied to integration of fuzzy logic with conventional techniques in encryption, which discuss possible benefits such as enhancement of security improvements when adaptability. The result of their research is that hybrid systems are quite useful as compared to the conventional techniques employed in cryptography, especially when you are doing it within an unplanned and unfixed environment.

IDEA's evolution and importance were developed to replace DES. It improved upon DES with a greater level of security due to its unique design and 128-bit key length. The design of IDEA incorporates eight rounds that work their intricate transformations, such as bitwise XOR operations, modular addition, and multiplication. These operations do provide nonlinearity and diffusion to IDEA that makes it immune against linear cryptanalysis (an attack that involves trying all possible keys with the same encryption key) as well differential cryptanalysis (a general form of an attack on a block cipher where pairs of plaintexts are encrypted with two similar but unknown keys). Several studies have evaluated the security and effectiveness of IDEA. For instance, the resistance of many varieties of attacks on IDEA was shown by Biham and Shamir [31] in a 1991 publication and Daemen and Rijmen [30] pointed out that IDEA was 'particularly secure' against them. Yet, the requirement for more secure methods increases with a rise in computing power. Against this backdrop, research is pursued into state-of-the-art techniques like soft cryptosystems aimed at the new classes of supercomputers with versatile hardware architectures. To explore the application of multi-polar interval-valued external neutrosophic hypersoft sets in decision-making problems under uncertainty along with distance, similarity measures, and machine learning by Saqlain et al. [32]. Another study by [33] focuses on uncertainties concerning crop economics and combines fuzzy hypersoft sets with the MULTIMOORA method and machine learning for a new way to enhance agricultural decision-making. Haq and Saqlain [34] provide an analysis of the adoption of machine learning methodologies for Sybil attack detection in IoT networks, emphasizing their effectiveness within unknown environments with a lack of information. Together, these insights have many implications for the construction of tools and decision-making frameworks in various areas such as agriculture or even cyber security.

## 2 | Preliminaries

In this section we define some useful definitions such as soft set and its relation with a matrix called soft matrix which is very helpful in computer programming by this we can store soft set in computer memory.

**Definition 1.** (Soft Set) [22]: Let $U$ be an initial universe and $\mathcal{P}(U)$ be the power set of $U, E$ be the set of all parameters, and $A \subseteq E$. $A$ soft set $(f_A, E)$ on the universe $U$ is defined by the set of ordered pairs which is given below:

$$(f_A, E) = \{(e, f_A(e)) : e \in E\}$$

where $f_A : E \to \mathcal{P}(U)$ such that $f_A(e) = \emptyset$ if $e \notin A$. Here $f_A$ is called the approximate function of the soft set $(f_A, E)$. The set $f_A(e)$ is called the e-approximate value set or e-approximate set which consists of related objects of the parameter $e \in E$.

**Definition 2.** (Soft Matrix) [23]: Let $U$ be the universal set and $(f_A, E)$ be a soft set over $U$. Then a subset of $U \times E$ is defined by:

$$R_A = \{(\mu, e): \mid e \in A, \mu \in f_A(e)\}$$

which is called a relation form of $(f_A, E)$.

The characteristic function of $R_A$ is written by:

$$\chi_{R_A}: U \times E \to [0,1]$$

$$\chi_{R_A}(\mu, e) = \begin{cases} 1, & \text{if } (\mu, e) \in R_A \\ 0, & \text{if } (\mu, e) \notin R_A \end{cases}$$

Where $R_A$ is the characteristic function. If $[a_{ij}] = \chi_{R_A}(\mu, e)$, then

$$[a_{ij}] = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}$$

is called the soft matrix of $(F, E)$ on $U$. Then all soft sets are denoted by $SM_{m\times n}$. **Example 1.** (Transformation of soft set into matrix): Assume that $U = \{u_1, u_2, u_3, u_4\}$ is a universal set and $E = \{e_1, e_2, e_3, e_4, e_5\}$ is a set of all parameters. If $A = \{e_1, e_2, e_3, e_5\}$, then

$$f_A(e_1) = \{u_1, u_3, u_4\},$$
$$f_A(e_2) = \{u_2, u_3, u_4\},$$
$$f_A(e_3) = \{u_1, u_2, u_3\}$$
$$f_A(e_5) = \{u_1, u_2, u_4\}$$

The corresponding soft set is $(f_A, E) = \{(e_1, \{u_1, u_3, u_4\}), (e_2, \{u_2, u_3, u_4\}), (e_3, \{u_1, u_2, u_3\}), (e_5, \{u_1, u_2, u_4\})\}$. The relation which is formed by $(f_A, E)$ is written as:

$$R_A = \{(u_1, e_1), (u_3, e_1), (u_4, e_1), (u_2, e_2), (u_3, e_2), (u_4, e_2), (u_1, e_3), (u_2, e_3), (u_3, e_3), (u_1, e_5), (u_2, e_5), (u_4, e_5)\}$$

Hence, the soft matrix is written by $[a_{ij}]$, taking set $U$ as the number of rows and set $E$ as the number of columns:

$$[a_{ij}] = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

**Definition 3**. (Inverse Product) [24]: Let $[a_{ij}], [b_{ij}] \in SM_{m\times n}$. The inverse product $i$ of $[a_{ij}]$ and $[b_{ij}]$ is defined as:

$$[a_{ij}] i [b_{ij}] = [c_{ij}]$$

where

$$c_{ij} = \begin{cases} 1, & \text{if } a_{ij} = b_{ij} \\ 0, & \text{if } a_{ij} \neq b_{ij} \end{cases}, \text{ for all } i, j.$$

**Definition 4.** (Characteristic Product): Let $[a_{ij}], [b_{ij}] \in SM_{m\times n}$. The characteristic product $^c$ of $[a_{ij}]$ and $[b_{ij}]$ is defined as:

$$[a_{ij}]^c [b_{ij}] = [c_{ij}]$$

where

$$c_{ij} = \begin{cases} 1, & \text{if } a_{ij} \neq b_{ij} \\ 0, & \text{if } a_{ij} = b_{ij} \end{cases}$$

for all $i, j$.

**Definition 5.** (IDEA) [15]: IDEA algorithm is an operator that operates on 64 blocks and uses 128-bit which consists of 8 identical transformations first round and as an output transformation in the second round. In the IDEA operator the process of encryption and decryption is the same.

**Definition 6**. (ASCII Code) [25]: This is used to represent text in computer language. ASCII, which stands for American Standard Code for Information Interchange, consists of many characters. It is a character encoding standard for electronic communication and is also helpful in telecommunication devices.

Here are some useful codes:

| | | |
|---|---|---|
| $A$ | 0001 | $A_1$ |
| $B$ | 0010 | $A_2$ |
| $C$ | 0011 | $A_3$ |
| $\vdots$ | $\vdots$ | $\vdots$ |
| $X$ | 1000 | $B_8$ |
| $Y$ | 1001 | $B_9$ |
| $Z$ | 1010 | $B_A$ |

**Example 2.** By using the definition of inverse product and characteristic product and by applying the IDEA operator, we can easily obtain. In this example take the key size (64-bit) and the 4 block size (16-bit). Now Jack wants to send a message to Rose, but they have not bad previous contact and the key does not want to take the time to send a courier with a key. Therefore, all information that Jack sends to Rose will potentially be obtained by the other person Wingston. However, it is still possible to send messages to be sent in such a way that Rose can read but Wingston cannot.

Jack and Rose have a soft set $(f_A, E)$ over $U = \{\mu_1, \mu_2, \mu_3, \mu_4\}$ and set of parameters $E = \{e_1, e_2, e_3, e_4\}$ which Wingston does not have information about. The soft set is given by:

$$(f_A, E) = \{(e_1, \{\mu_2, \mu_3, \mu_4\}), (e_2, \{\mu_1, \mu_2, \mu_4\}), (e_3, \{\mu_2, \mu_3\})\}$$

## 3 | Process of Encryption

**Step 1.** Let Jack and Rose have a soft set $(f_A, E)$ given by:

$$(f_A, E) = \{(e_1, \{\mu_2, \mu_3, \mu_4\}), (e_2, \{\mu_1, \mu_2, \mu_4\}), (e_1, \{\mu_2, \mu_3\})\}$$

**Step 2.** The soft matrix $S$ corresponding to the soft set $(f_A, E)$ is given by:

$$S = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

**Step 3.** Now Jack has a message of 64-bit which is "SOLVED ENCRYPTION".Make section of this message into 4 parts SOLV-EDEN-CRYP-TION. By using ASCII code numerical value we have:

$$\text{SOLV } = 0011{,}1111{,}1100{,}0110, \quad K_1 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix},$$

$$\text{EDEN } = 0101{,}0100{,}0101{,}1110, \quad K_2 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix},$$

$$\text{CRYP } = 0011{,}0010{,}1001{,}0000, \quad K_3 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix},$$

$$\text{TION } = 0100{,}1001{,}1111{,}1110, \quad K_4 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

**Step 4.** Now we have to suppose $\alpha$ permutation such that each column of the soft matrix will be rearranged according to the $\alpha$ after permuting we obtain $S_\alpha$ as the key which we obtain after permutation

Let

- For $\alpha_1 = (1432)$ :
- For $\alpha_2 = (1342)$ :
- For $\alpha_3 = (2143)$ :
- For $\alpha_4 = (3142)$ :

  for all $\in S$

So each column of soft matrix S will be rearranged according to $\alpha$

$$1 \rightarrow 4 \rightarrow 3 \rightarrow 2 \rightarrow 1$$

By applying the permutation $\alpha_1$, we obtain $S_{\alpha_1}$ as follows:

$$S_{\alpha_1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

Similarly, by applying the other permutations, we have:

$$S_{\alpha_2} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

$$S_{\alpha_3} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

$$S_{\alpha_4} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

**Step 5.** Now we apply the inverse and characteristic production we get the cipher result.

$$K_1 \cdot iS_{\alpha_1} \to C_1$$
$$K_2 \cdot cS_{\alpha_2} \to C_2$$
$$K_3 \cdot cS_{\alpha_3} \to C_3$$
$$K_4 \cdot iS_{\alpha_4} \to C_4$$

$$K_1 \cdot iS_{\alpha_1} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \cdot i \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} = C_1$$

$$K_2 \cdot cS_{\alpha_2} = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \cdot i \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} = C_2$$

$$K_3 \cdot cS_{\alpha_3} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \cdot i \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} = C_3$$

$$K_4 \cdot iS_{\alpha_4} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \cdot i \cdot \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix} = C_4$$

After ASCII code we have the following values according to the obtained matrices.

$$\mathrm{C_1 = KDOOC_2 = BELYC_3 = DFEFC_4 = FNJM}$$

**Step 6.** This time to rearranged the letters that we obtained by ASCII code. We have to convert these letters into sentences and will be sent by Jack to Rose even Wingston gets this sentence but he cannot know the message which is given by Jack. The sentence becomes "KDOOBELYDFEFFNJM" and this will be received by Rose. The flowchart of the process of encryption is listed below for better understanding in Figure 1.

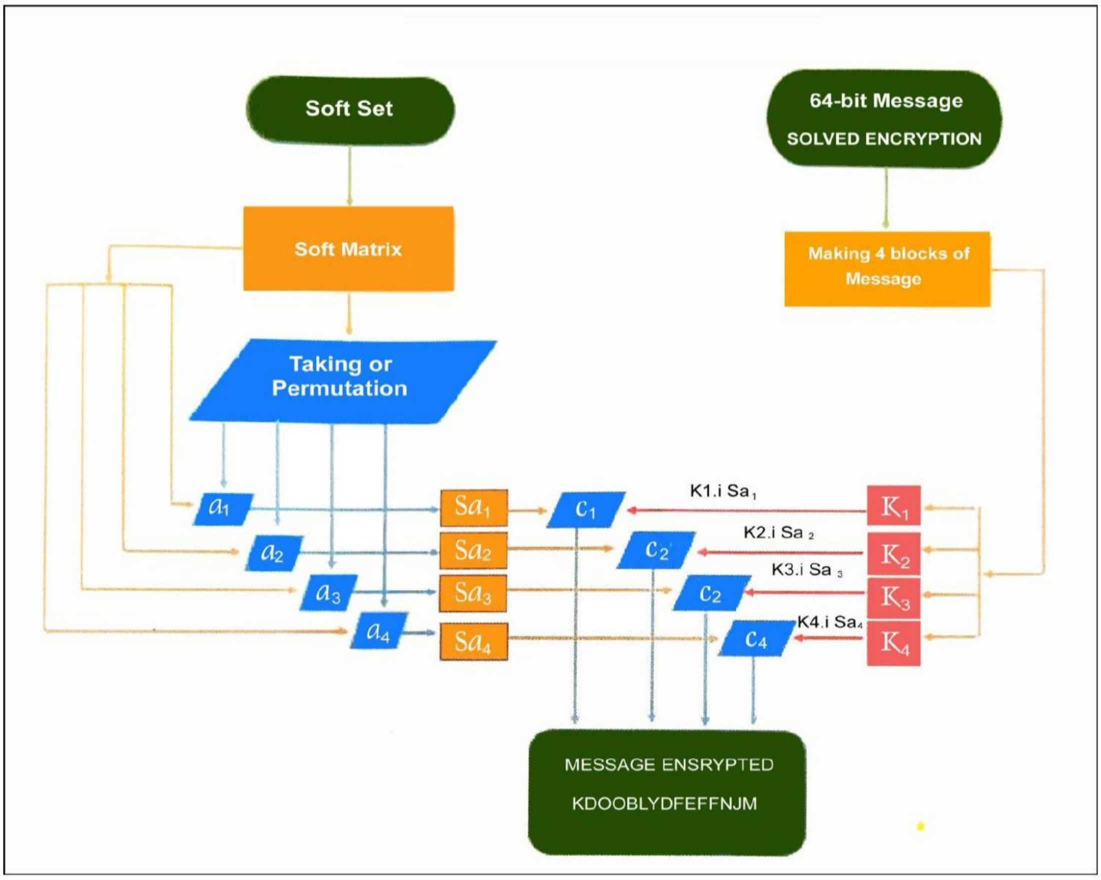

**Figure 1.** Flowchart of encryption.

## 4 |Process Of Decryption

**Step 1.** Now Rose takes the same soft set which is:

$$(f_A, E) = \{(e_1, \{\mu_2, \mu_3, \mu_4\}), (e_2, \{\mu_1, \mu_2, \mu_4\}), (e_1, \{\mu_2, \mu_3\})\}$$

**Step 2.** The soft matrix corresponding to the soft set will be.

$$S = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

**Step 3.** In this step, we take the message "KDOOBELYDFEFFNJM". Now make sections of this message into 4 parts KDOO-BELY-DFEF-FNJM. By using ASCII code we have a numerical value of these four sections. KDOO-1011,0100,1111,1111

$$C_1 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

BELY-0010,0101,1100,1001

$$C_2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

DFEF- 0100,0110,0101,0110

$$C_3 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

FNJM- 0110,1110,1010,1101

$$C_4 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$

**Step 4.** Now we have to suppose $\alpha$ permutation such that each column of the soft matrix will be rearranged according to the $\alpha$ after permuting. We obtain $S_\alpha$ as key which we obtained after permutation.

Let

- For $\alpha_1 = (1432)$:
- For $\alpha_2 = (1342)$:
- For $\alpha_3 = (2143)$:
- For $\alpha_4 = (3142)$:

  for all $\in S$

So each column of soft matrix S will be rearranged according to $\alpha$ $1 \rightarrow 4 \rightarrow 3 \rightarrow 2 \rightarrow 1$

By applying the permutation $\alpha_1$, we obtain $S_{\alpha_1}$ as follows:

$$S_{\alpha_1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

Similarly, by applying the other permutations, we have:

$$S_{\alpha_2} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

$$S_{\alpha_3} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

$$S_{\alpha_4} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

**Step 5.** Now applying the inverse and characteristic production we got the cypher result.

$$C_1 \cdot iS_{\alpha_1} \rightarrow K_1$$
$$C_2 \cdot cS_{\alpha_2} \rightarrow K_2$$
$$C_3 \cdot cS_{\alpha_3} \rightarrow K_3$$
$$C_4 \cdot iS_{\alpha_4} \rightarrow K_4$$

$$C_1 \cdot iS_{\alpha_1} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \cdot_{i} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} = K_1$$

$$C_2 \cdot cS_{\alpha_2} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \cdot_{i} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} = K_2$$

$$C_3 \cdot cS_{\alpha_3} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \cdot i \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} = K_3$$

$$C_4 \cdot iS_{\alpha_4} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix} \cdot_{i} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} = K_4$$

**Step 6.** These obtained matrices will give us the original message that is being sent by Jack to Rose "SOLVED ENCRYPTION". On the same basis, they can also share messages which are lesser or greater than 16 letters by using empty spaces and taking (0000)as an ASCII code against empty spaces.

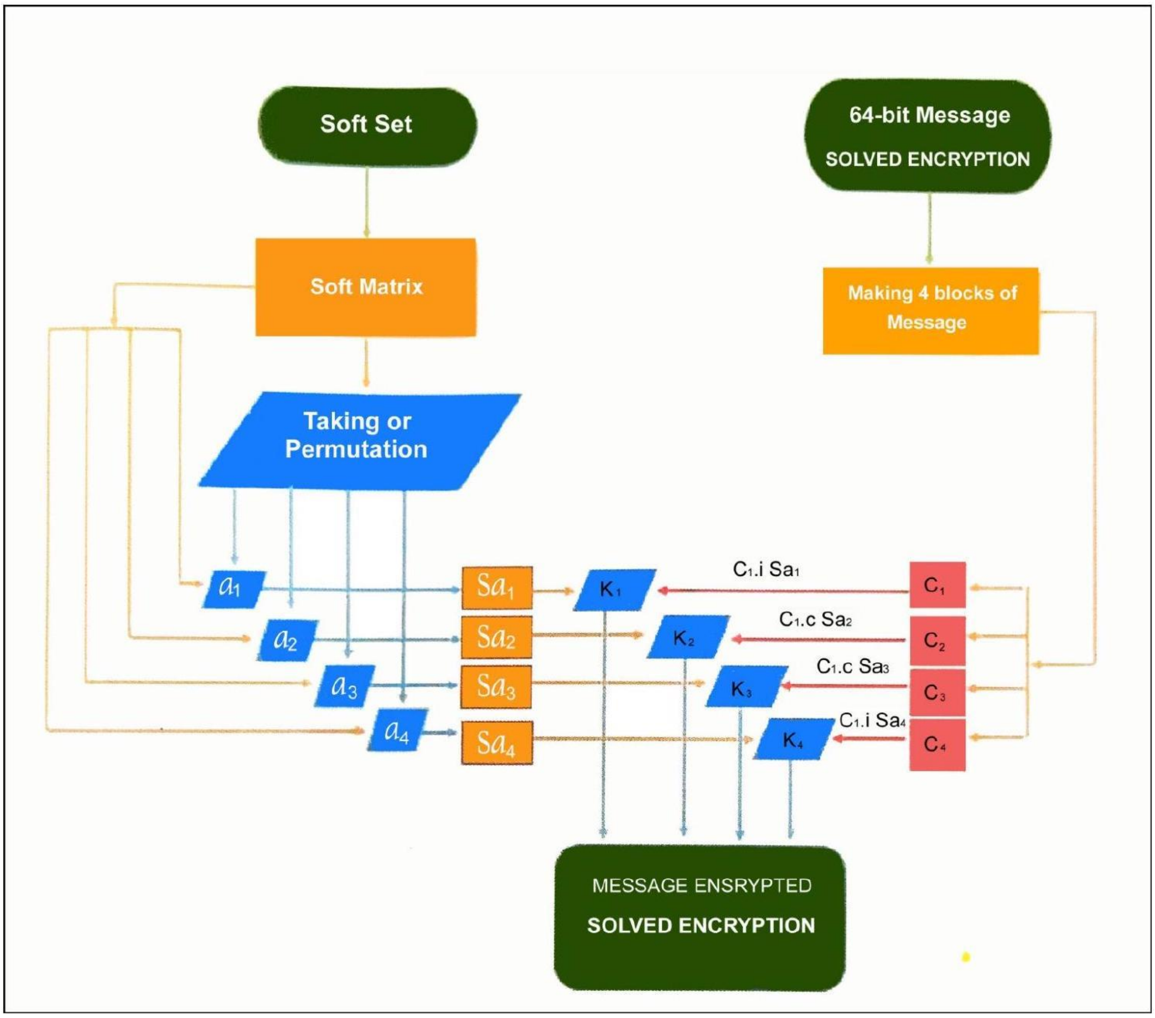

**Figure 2.** Flowchart of decryption.

## 5 |Conclusions

Encryption and unscrambling is a cryptosystem substantial for moving privileged data. An exact and special strategy has been utilized in this paper that IDEA is applied on a soft set after changed over into a soft matrix by then the definition of inverse and characteristic product is applied to the soft matrix and 4 soft matrices of message at that point message is encrypted and can be shipped off inverse. On applying the same technique for the Decryption receiver will get the message.

Furthermore, the size of the soft matrix changes according to taking suitable bits of message and can also do the operation in the rows instead of the columns.

## 6 |Future Guides

i). Enhanced Security: Integrate additional security layers, such as quantum-resistant algorithms, to strengthen the cryptosystem.

ii). Optimization: Improve computational efficiency, particularly for real-time applications and resource-constrained environments.

iii). Scalability: Develop scalable versions that adapt to varying security needs and data sizes.

iv). Variations: Explore different fuzzy logic paradigms or encryption algorithms within the soft cryptosystem.

v). Emerging Technologies: Implement the cryptosystem on platforms like blockchain and cloud computing.

vi). User Accessibility: Enhance user interface and accessibility for non-experts.

vii). Comparative Analysis: Benchmark the cryptosystem against established cryptographic techniques.

viii). Regulatory Compliance: Ensure alignment with data protection laws and ethical considerations.

ix). Industry Adaptation: Customize the cryptosystem for specific industries like healthcare or finance.

x). AI Integration: Incorporate AI to dynamically adjust encryption strategies based on threat analysis.

## Acknowledgments

The author is grateful to the editorial and reviewers, as well as the correspondent author, who offered assistance in the form of advice, assessment, and checking during the study period.

## Author Contributions

All authors contributed equally to this work.

## Funding

This research was conducted without external funding support.

## Data Availability

The datasets generated during and/or analyzed during the current study are not publicly available due to the privacy-preserving nature of the data but are available from the corresponding author upon reasonable request.

## Conflicts of Interest

The author declares that there is no conflict of interest in the research.

## Ethical Approval

This article does not contain any studies with human participants or animals performed by any of the authors.

# References

[1] M. Arshad, M. Saeed, and A. U. Rahman, "A novel intelligent multi-attributes decision-making approach based on generalized neutrosophic vague hybrid computing," Neutrosophic Sets and Systems, vol. 50, pp. 532-551, 2022.

[2] M. Saqlain and M. Saeed, "From ambiguity to clarity: unraveling the power of similarity measures in multi-polar interval-valued intuitionistic fuzzy soft sets," Decision Making Advances, vol. 2, no. 1, pp. 48-59,2024.

[3] R. C. Lee, "Fuzzy logic and the resolution principle," Journal of the ACM (JACM), vol. 19, no. 1, pp. 109-119, 1972.

[4] M. Saeed, M. Hussain, and A. A. Mughal, "A study of soft sets with soft members and soft elements: A new approach," Punjab University Journal of Mathematics, vol. 52, no. 8, 2020.

[5] S. R. Shinge and R. Patil, "An encryption algorithm based on ascii value of data," International Journal of Computer Science and Information Technologies, vol. 5, no. 6, pp. 7232-7234, 2014.

[6] U. Rahman, M. Saeed, M. H. Saeed, D. A. Zebari, M. Albahar, K. H. Abdulkareem, A. S. Al-Waisy, and M. A. Mohammed, "A framework for susceptibility analysis of brain tumours based on uncertain analytical cum algorithmic modeling," Bioengineering, vol. 10, no. 2, p. 147, 2023.

[7] S. Yasin, K. Haseeb, and R. J. Qureshi, "Cryptography based e-commerce security: a review," International Journal of Computer Science Issues (IJCSI), vol. 9, no. 2, p. 132, 2012.

[8] P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh, and W.-C. Hong, "Internet of things: Evolution, concerns and security challenges," Sensors, vol. 21, no. 5, p. 1809, 2021.

[9] E. Manpearl, "Preventing going dark: A sober analysis and reasonable solution to preserve security in the encryption debate," U. Fla. JL & Pub. Pol'y, vol. 28, p. 65, 2017.

[10] J. Nakahara Jr, "Lai-massey cipher designs," History, Design Criteria and Cryptanalysis.

[11] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, "Twofish: A 128-bit block cipher," NIST AES Proposal, vol. 15, no. 1, pp. 23-91, 1998.

[12] O. Almasri and H. M. Jani, "Introducing an encryption algorithm based on idea," International Journal of Science and Research (IJSR), India, vol. 2, no. 9, 2013.

[13] L. A. Zadeh, G. J. Klir, and B. Yuan, Fuzzy sets, fuzzy logic, and fuzzy systems: selected papers, vol. 6. World scientific, 1996.

[14] E. Aygün, "Soft matrix product and soft cryptosystem," Filomat, vol. 32, no. 19, pp. 6519-6530, 2018.

[15] W. G. Júnior and D. P. Júnior, "A proposal of a cryptography algorithm with techniques of error correction," Computer Communications, vol. 20, no. 15, pp. 1374-1380, 1997.

[16] X. Lai, J. L. Massey, and Murphy, S. Markov ciphers and differential cryptanalysis. In Advances in Cryptology—EUROCRYPT' 91: Workshop on the Theory and Application of Cryptographic Techniques Brighton, UK, April 8–11, 1991 Proceedings 10 (pp. 17-38). Springer Berlin Heidelberg, 1991.

[17] M .Zulqarnain and M Saeed, A new decision making method on interval valued fuzzy soft matrix (IVFSM). British Journal of Mathematics & Computer Science, 20(5), 1-17 (2017).

[18] S. K. Langford and M. E. Hellman, "Differential-linear cryptanalysis," in Advances in Cryptology-CRYPTO'94: 14th Annual International Cryptology Conference Santa Barbara, California, USA August 21-25, 1994 Proceedings 14, pp. 17-25, Springer, 1994.

[19] R. L. Rivest, "Cryptography," in Algorithms and complexity, pp. 717-755, Elsevier, 1990.

[20] S. Basu, "International data encryption algorithm (idea)-a typical illustration," Journal of global research in Computer Science, vol. 2, no. 7, pp. 116-118, 2011.

[21] S. Gupta, "Encryption and decryption," International Journal of Managment, IT and Engineering, vol. 2, no. 8, pp. 441-459, 2012.

[22] D. Molodtsov, "Soft set theory—first results," Computers & mathematics with applications, vol. 37, no. 4-5, pp. 19-31, 1999.

[23] M. Tierz, "Soft matrix models and chern-simons partition functions," Modern Physics Letters A, vol. 19, no. 18, pp. 1365-1378, 2004.

[24] D. Benjamin, "Can unobserved land quality explain the inverse productivity relationship?," Journal of Development Economics, vol. 46, no. 1, pp. 51-84, 1995.

[25] E. Kaier and E. Kaier, "Ascii-code," Turbo Pascal 6.0: Griffbereit, pp. 96-96, 1991.

[26] L.A. Zadeh, Fuzzy sets. Information and control, 8(3), 338-353, 1965.

[27] Zhu, A. X., Yang, L., Li, B., Qin, C., Pei, T., and Liu, B. Construction of membership functions for predictive soil mapping under fuzzy logic. Geoderma, 155(3-4), 164-174, 2010.

[28] Kumar, P., Gupta, G. P., & Tripathi, R. Toward design of an intelligent cyber attack detection system using hybrid feature reduced approach for iot networks. Arabian Journal for Science and Engineering, 46(4), 3749-3778, 2021.

[29] N. A. Patel, D. A. Parekh, A. Y. Shah, and R. Mangrulkar, 4S Framework: A Practical CPS Design Security Assessment and Benchmarking Framework. Cyber Security and Digital Forensics, 163-204, 2022.

[30] E. Oswald, J. Daemen, and V. Rijmen, Aes-the state of the art of rijndael's security, 2002.

[31] E. Biham, and A.Shamir, Differential fault analysis of secret key cryptosystems 513-525,1997.

[32] M. Saqlain, H. Garg, P. Kumam, W. Kumam. "Uncertainty and decision-making with multi-polar interval-valued neutrosophic hypersoft set: A distance, similarity measure, and machine learning approach." Alexandria Engineering journal, vol. 84, pp. 323-332, 2023. https://doi.org/10.1016/j.aej.2023.11.001

[33] M. Saqlain, P. Kumam, W. Kumam. "Uncertainty and Decision-Making in Crop Economics Using Fuzzy Hypersoft Set with MULTIMOORA Method and Machine Learning." In: Ngoc Thach, N., Trung, N.D., Ha, D.T., Kreinovich, V. (eds) Partial Identification in Econometrics and Related Topics. Studies in Systems, Decision and Control, vol 531. Springer, Cham. https://doi.org/10.1007/978-3-031-59110-5_5

[34] H. B. ul Haq & M. Saqlain. "An Implementation of Effective Machine Learning Approaches to Perform Sybil Attack Detection (SAD) in IoT Network." Theoretical and Applied Computational Intelligence , vol. 1, no 1, pp. 1-14, 2023. https://doi.org/10.31181/taci1120232

**Disclaimer/Publisher's Note:** The perspectives, opinions, and data shared in all publications are the sole responsibility of the individual authors and contributors, and do not necessarily reflect the views of Sciences Force or the editorial team. Sciences Force and the editorial team disclaim any liability for potential harm to individuals or property resulting from the ideas, methods, instructions, or products referenced in the content.