In the Name of God

Journal of
Information Systems & Telecommunication
Vol. 12, No.3, July-September 2024, Serial Number 47

Research Institute for Information and Communication Technology
Iranian Association of Information and Communication Technology
Affiliated to: Academic Center for Education, Culture and Research (ACECR)

Manager-in-Charge: Dr. Habibollah Asghari, ACECR, Iran
Editor-in-Chief: Dr. Masoud Shafiee, Amir Kabir University of Technology, Iran

Editorial Board
Dr. Abdolali Abdipour, Professor, Amirkabir University of Technology, Iran
Dr. Ali Akbar Jalali, Professor, Iran University of Science and Technology, Iran
Dr. Alireza Montazemi, Professor, McMaster University, Canada
Dr. Ali Mohammad-Djafari, Associate Professor, Le Centre National de la Recherche Scientifique (CNRS), France
Dr. Hamid Reza Sadegh Mohammadi, Associate Professor, ACECR, Iran
Dr. Mahmoud Moghavvemi, Professor, University of Malaya (UM), Malaysia
Dr. Mehrnoush Shamsfard, Associate Professor, Shahid Beheshti University, Iran
Dr. Omid Mahdi Ebadati, Associate Professor, Kharazmi University, Iran
Dr. Rahim Saeidi, Assistant Professor, Aalto University, Finland
Dr. Ramezan Ali Sadeghzadeh, Professor, Khajeh Nasireddin Toosi University of Technology, Iran
Dr. Sha'ban Elahi, Associate Professor, Tarbiat Modares University, Iran
Dr. Shohreh Kasaei, Professor, Sharif University of Technology, Iran
Dr. Saeed Ghazi Maghrebi, Assistant Professor, ACECR, Iran
Dr. Zabih Ghasemlooy, Professor, Northumbria University, UK

Executive Editor: Dr. Fatemeh Kheirkhah
Executive Manager: Shirin Gilaki
Executive Assistants: Mahdokht Ghahari, Ali BoozarPoor
Print ISSN: 2322-1437
Online ISSN: 2345-2773
Publication License: 91/13216
Editorial Office Address: No.5, Saeedi Alley, Kalej Intersection., Enghelab Ave., Tehran, Iran,
P.O.Box: 13145-799 Tel: (+9821) 88930150 Fax: (+9821) 88930157
E-mail: info@jist.ir , infojist@gmail.com
URL: www.jist.ir

Indexed by:
- SCOPUS www. Scopus.com
- Index Copernicus International www.indexcopernicus.com
- Islamic World Science Citation Center (ISC) www.isc.gov.ir
- Directory of open Access Journals www.Doaj.org
- Scientific Information Database (SID) www.sid.ir
- Regional Information Center for Science and Technology (RICeST) www.ricest.ac.ir
- Magiran www.magiran.com

Publisher:
Iranian Academic Center for Education, Culture and Research **(ACECR)**

This Journal is published under scientific support of
Advanced Information Systems (AIS) Research Group and
Telecommunication Research Group, ICTRC

Acknowledgement

JIST Editorial-Board would like to gratefully appreciate the following distinguished referees for spending their valuable time and expertise in reviewing the manuscripts and their constructive suggestions, which had a great impact on the enhancement of this issue of the JIST Journal.

(A-Z)

- Afsharirad, Majid, Kharazmi University,Tehran, Iran
- Arzilawati , Nur, Universiti Putra Malaysia, Selangor, Malaysia
- Azarkasb, Seyed Omid, K.N. Toosi University of Technology, Tehran, Iran
- Entezari Maleki, Reza, Iran University of Science and Technology (IUST), Tehran, Iran
- Fadaeieslam, Mohammad Javad, Semnan University, Iran
- Fakhar, Fatemeh, Payame Noor University, Ahvaz, Iran
- Farsi, Hassan, University of Birjand, South Khorasan, Iran
- Farsijani, Hassan, Shahid Beheshti University, Tehran, Iran
- Ghaffari, Hamidreza, Ferdous Azad University, South Khorasan Province, Iran
- Junayed, Hasan, Universiteit van Ulsan, Ulsan, South Korea
- Kasaei, Shohreh, Sharif University, Tehran, Iran
- Kashef, Seyed Sadra, Urmia University, Urmia, Iran
- Kolahkaj, Maral, Islamic Azad University, Karaj Branch, Iran
- Mavadati, Samira, Mazandaran University, Mazandaran, Iran
- Mohammadzadeh, Sajjad, University of Birjand, South Khorasan, Iran
- Moayedi, Fatemeh, University of Larestan Higher Education Complex, Fars, Iran
- Omid Mahdi, Ebadati, Kharazmi University, Tehran, Iran
- Pujo Hari, Saputro, University of Sam Ratulangi, Manado, Indonesia
- Soleimanian Gharehchopogh, Farhad, Islamic Azad University Urmia, Iran
- Tanhaei, Mohammad, Ilam University, Ilam, Iran
- Tourani, Mahdi, University of Birjand, South Khorasan, Iran
- Valizadeh, Majid, Ilam University, Ilam, Iran
- Vahidipour, Mahdi, Amirkabir University of Technology, Tehran, Iran
- Zahedi, Mohammad Hadi, K. N. Toosi University of Technology, Tehran, Iran

Table of Contents

- **Elymus Repens Optimization (ERO); A Novel Agricultural-Inspired Algorithm 170**

Mahdi Tourani

- **Enhancing IoT Security: A Comparative Analysis of Hybrid Hyperparameter Optimization for Deep Learning-Based Intrusion Detection Systems 183**

Heshmat Asadi, Mahmood Alborzi and Hesam Zandhesami

- **A Survey of Intrusion Detection Systems Based On Deep Learning for IoT Data 197**

Mehrnaz Moudi, Arefeh Soleimani and Amir Hossein Hojjatinia

- **Improving Opinion Mining Through Automatic Prompt Construction 208**

Arash Yousefi Jordehi, Mahsa Hosseini Khasheh Heyran, Saeed Ahmadnia, Seyed Abolghasem Mirroshandel and Owen Rambow

- **Economic Impacts and Global Successes through the Internet of Everything (IoE) in the World Countries 220**

Seyed Omid Azarkasb and Seyed Hossein Khasteh

- **GOA-ISR: A Grasshopper Optimization Algorithm for Improved Image Super-Resolution 233**

Hamid Azad, Bahar Ghaderi and Hamed Agahi

Journal of Information Systems and Telecommunication
Vol.12, No.3,July-September 2024, 170-182
http://jist.acecr.org
ISSN 2322-1437 / EISSN:2345-2773

Elymus Repens Optimization (ERO); A Novel Agricultural-Inspired Algorithm

Mahdi Tourani[1*]

[1]. Faculty of Engineering, University of Birjand

Received: 01 Apr 2023/ Revised: 27 July 2024/ Accepted: 20 Aug 2024

Abstract

Optimization plays a crucial role in enhancing productivity within the industry. Employing this technique can lead to a reduction in system costs. There exist various efficient methods for optimization, each with its own set of advantages and disadvantages. Meanwhile, meta-heuristic algorithms offer a viable solution for achieving the optimal working point. These algorithms draw inspiration from nature, physical relationships, and other sources. The distinguishing factors between these methods lie in the accuracy of the final optimal solution and the speed of algorithm execution. The superior algorithm provides both precise and rapid optimal solutions. This paper introduces a novel agricultural-inspired algorithm named Elymus Repens Optimization (ERO). This optimization algorithm operates based on the behavioral patterns of Elymus Repens under cultivation conditions. Elymus repens is inclined to move to areas with more suitable conditions. In ERO, exploration and exploitation are carried out through Rhizome Optimization Operator and Stolon Optimization Operators. These two supplementary activities are used to explore the problem space. The potent combination of these operators, as presented in this paper, resolves the challenges encountered in previous research related to speed and accuracy in optimization issues. After the introduction and simulation of ERO, it is compared with popular search algorithms such as Gravitational Search Algorithm (GSA), Grey Wolf Optimizer (GWO), Particle Swarm Optimization (PSO), and Firefly Algorithm (FA). The solution of 23 benchmark functions demonstrates that the proposed algorithm is highly efficient in terms of accuracy and speed.

Keywords: Elymus Repens Optimization; Meta-Heuristic Algorithms; Rhizome Optimization Operator; Stolon Optimization Operator.

1- Introduction

Today, the industry faces various pressing problems that require urgent solutions and optimal answers. Contributing to the resolution of these issues can greatly enhance efficiency across multiple fields. There exist diverse approaches to solving optimization problems, including one-by-one counting methods, classical mathematical methods, and optimization methods.

The one-by-one method involves a significant amount of time to solve problems, rendering it practical only for small-scale issues. However, its advantages encompass very high accuracy and zero error.

Conversely, classical mathematical methods, such as derivation methods, require adherence to specific principles and rules for continuous problems. These limitations can make it challenging to employ these methods for solving optimization problems. Nonetheless, classical mathematical methods offer high accuracy, making them an appealing option.

In optimization methods, algorithms begin in an initial space and move intelligently towards an optimal solution. With effective guiding operators, these algorithms conduct smarter searches in problem spaces, ultimately accelerating the process of reaching a final answer. Several desirable features of optimization methods include:

- No limitation in problem modeling
- Universality in covering a wide range of issues
- High speed in determining the optimal answer

In this paper, a powerful method is introduced for optimizing problems by harnessing the positive features of nature to address challenges. One such valuable feature is the growth mechanism of Elymus repens in agricultural land, which provides an innovative approach to problem-solving.

The paper proceeds as follows: Section 2 provides an overview of optimization algorithms. Section 3 introduces the Elymus repens mechanism, and Section 4 presents the new algorithm called Elymus repens optimization. Finally, in Section 5, the performance of this new algorithm is evaluated using 23 sample functions.

✉**Mahdi Tourani**
tourani.mahdi@birjand.ac.ir

2- Literature review

Today, optimization algorithms are used as a method for obtaining the optimal solutions to optimization problems[1]. Unlike classical mathematical methods, these algorithms are much more efficient in solving optimization problems. The basis of optimization algorithms is usually nature, physics, and swarm. The final answer obtained from them has high accuracy and suitable speed. Optimization algorithms use two basic components of exploration and exploitation to search the problem space. These two features are very helpful in finding the optimal answer. Exploration provides the algorithm with the ability to search freely without paying attention to the accuracy of the results. On the other hand, paying attention to the information obtained in the previous loops is the basis of exploitation. With an increase of exploration, the algorithm finds random and unpredictable directions, and on the opposite side, with an increase of exploitation, the performance of the algorithm becomes cautious. By the exploration and exploitation, the algorithm will move towards the smart answer.

In the following, some of the popular optimization algorithms are reviewed [2]:

Genetic Algorithm [3], Genetic programming [4], Tabu Search [5], Evolution Strategy [6], Memetic Algorithm [7], Cultural Algorithm [8], Simulated Annealing [9], Differential Evolution [10], Evolutionary Programming [11], Co Evolutionary Algorithm [12], Gradient Evolution Algorithm [13], Imperialistic Competitive Algorithm [14], Biogeography-Based Optimization [15], States of Matter Search [16], Sine Cosine Algorithm [17], Multi-level Cross Entropy Optimizer [18]. These algorithms are modeled on Darwin's theories.

Some algorithms are physics-based optimization algorithms such as: Small-World Optimization Algorithm [19], Central Force Optimization [20], Magnetic Optimization Algorithm [21], Gravitational Search Algorithm [22], Charged System Search [23], Chemical-Reaction Optimization [24], Black Hole [25], Curved Space Optimization [26], Water Evaporation Optimization [27], Ideal Gas Molecular Movement [28], Multi-Verse Optimizer [29], Vibrating Particles System [30].

Some optimizers are swarm-based algorithms: Particle Swarm Optimization [31], Grasshopper Optimization Algorithm [32], Moth–flame Optimization [33], Artificial Fish Swarm Algorithm [34], Honey Bee Optimization [35], Termite Colony Optimization [36], Ant Colony Optimization [37], Shuffled Frog-Leaping [38], Monkey Search [39], Dolphin Partner Optimization [40], Firefly Algorithm [41], Bat Algorithm [1], Bird Mating Optimizer [42], Fruit Fly Optimization [43], Lion Pride Optimizer [44], Krill Herd [45], Grey Wolf Optimizer [46], Cuckoo Search [47], Soccer League Competition Algorithm [48], Dragonfly Algorithm [49], Whale Optimization Algorithm [50], Salp Swarm Algorithm [51], Harris Hawks Optimization [52], Flying Squirrel Optimizer [53], Ant Lion Optimizer [54]

In addition to these algorithms, some intelligence may be found in nature that can form the basis of other optimization algorithms. One of these is the Elymus Repens behavior.

The introduced algorithms are very effective in industry, energy, medicine and etc. References [55-59] in science, [60-64] in engineering and [65-69] in medical show part of the research conducted with these algorithms in the field of optimization.

3- Elymus Repens

Elymus repens (ER) is a highly competitive, allelopathic, perennial grass. This plant is considered one of the world's most troublesome weeds, reproducing both sexually through seeds and asexually through rhizomes. It is found in temperate regions worldwide, with the exception of Antarctica [70, 71, 72]. The structure and appearance of this plant are depicted in Fig. 1 and Fig. 2.

In Northern Europe, Elymus repens is a common and aggressive grass species favored by cereal-dominated crop rotations and nitrogen fertilization [73, 74]. This species can become a pernicious weed, spreading rapidly by underground rhizomes[72] and quickly forming a dense mat of roots in the soil. Even the smallest fragment of the root can regenerate into a new plant[75].

Elymus repens is propagated by seeds, rhizomes, or stolons. The creeping stems on the ground surface and the wire-shaped underground stems have numerous short branches and scaly leaves. New aerial organs are formed from the nodes of rhizomes and stolons.

This plant is highly resilient and can thrive in favorable conditions on the ground. These conditions include water, organic, and biological materials. Where these conditions are optimal, the growth of this plant flourishes. On the other hand, this plant can be considered as a "search engine" as it moves towards favorable agricultural positions and covers them using propagation tools such as rhizomes or stolons. Once introduced to an area, it swiftly moves to better conditions and occupies the desired area.

The power and speed of occupying fertile areas by this plant is so high that it prevents the growth of any other type of plant, thus making it one of the most destructive weeds.



Fig. 1. Elymus Repens [76]



Fig. 2. Elymus Repens in the agricultural land

4- Elymus Repens Optimization

This study is centered around the behavior patterns of Elymus Repens within their cultivation environment. In terms of growth and reproduction, this plant initially progresses through seeds and subsequently through rhizomes and stolons (illustrated in Fig. 3) within the cultivation environment. Elymus repens tends to move towards any part of the soil that provides more favorable conditions.

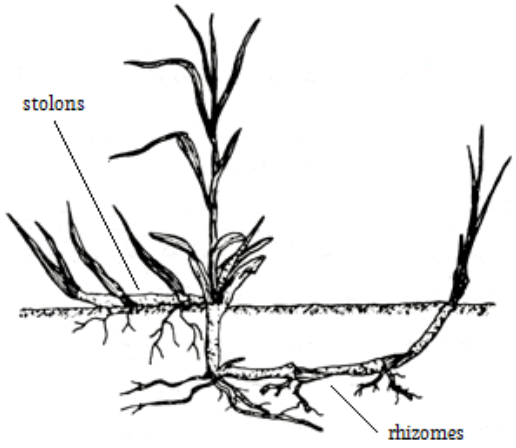


Fig. 3.Rhizomes and Stolons in Elymus Repens

In this paper, this process is modeled as a optimization search algorithm that is named Elymus Repens Optimization (ERO). In the ERO model, the cultivation land of the plant serves as the search space for the problem, with every position within this space being a candidate answer - representing a position of the land with the best cultivation conditions, i.e., the optimal answer. The rhizomes and stolons act as the ERO optimization operators.

To initiate the algorithm, Elymus repens is assumed to be spread across the environment. Any position in the cultivation environment where the reproductive parts of the plant are placed becomes an initial candidate answer. These positions are evaluated using the objective function. Subsequently, the Elymus repens will move towards the optimal answer through the use of rhizomes and stolons.

4-1- Stolon Optimization Operator

Among the reproducible parts of Elymus repens, the part that is in a better environmental condition will spread to its neighboring parts through stolons. The number of neighbors for each position will increase with the improved environmental conditions. Consequently, a part of the plant that is in unfavorable conditions will not be reproduced. This process guides the initial solution towards better alternatives. Equation 1 and Equation 2 demonstrate the new candidate solutions with the stolon operator.

$$\alpha = \beta(1-\frac{it}{T}) \tag{1}$$

$$X_{i\in neighbor}^{k,it} = X_{k\in best}^{it-1} + unifrnd(-\alpha,+\alpha) \tag{2}$$

where, *it* indicates iteration, *T* the maximum of iteration, $X_{i\in neighbor}{}^{kit}$ show *i-th* neighbor from *k-th* best position, $X_{k\in best}{}^{it\text{-}1}$ the *k-th* best choice position, *unifrnd*, a uniform

random number between [-α,+α] and β is the relationship coefficient.

The best position ($X_{i \in best}$) for reproduction is selected using the roulette wheel. This method ensures that better positions have a higher chance of reproducing. This selection process is repeated for all positions, and the resulting new neighbors are generated from the best ones.

4-2- Rhizome Optimization Operator

In 4-1, the k-best position of population generate a number of neighbors. The neighbors related to each k-best position form a group. At this step, in each group, the best neighbor is selected from among the neighbors created by each previous k-best position, and the other neighbors move towards it. Equations 3 to 6 show the new candidate solutions using the rhizome operator.

$$A = \beta \times \alpha \times rand - \alpha \quad (3)$$

$$C = \beta \times rand \quad (4)$$

$$D_i^k = abs(\mathrm{C} \times X_{best\ neighbor}^{k,it-1} - X_{i \in other\ neighbor}^{k,it-1}) \quad (5)$$

$$X_i^{it} = X_{best\ neighbor}^{k,it-1} - A \times D_i^k \quad (6)$$

where, X_i^{it} *is new* candidate answer, rand shows the random value between [0,1] and $X_{best\ neighbor}^{k,it-1}$ and $X_{i \in other\ neihbor}^{kit-1}$, are the best neighbor and other neighbors for *k-th* neighborhood group. Fig. 4 shows the visual performance of rhizomes and stolons operators in ER optimization.

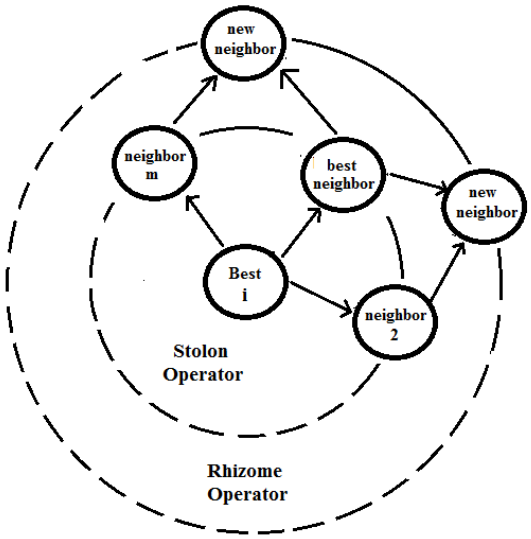


Fig. 4. The stolon and rhizome operators view

The flowchart and the pseudo code of ERO algorithm are presented in Fig. 5 and Fig. 6.

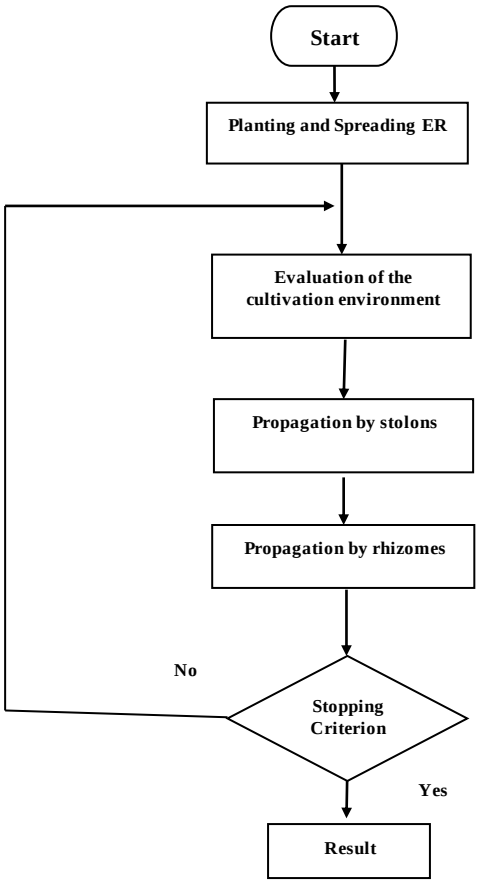


Fig. 5. Flowchart of the Proposed ERO Algorithm

Step 1: Planting the elymus repen and spreading it in the cultivation environment
Step 2: Evaluation of the cultivation environment
Step 3: Propagation of the elymus repen by stolons
Step 4: Propagation of the elymus repen by rhizomes
Step 5: if stop criteria has not been reached, Go to step 2.

Fig. 6. The pseudo code of ERO algorithm

5- Validation and Computational Experiment

To demonstrate the effectiveness and power of Elymus Repens Optimization as proposed in this paper, it has been evaluated for minimizing 23 case study functions [77]. Table 2 depicts these well-known functions. For the computational testing, the simulations were run on a PC with a 2.30GHz Intel Core i5 processor and 6 gigabytes of RAM.

The aim of the algorithm presented is to minimize the functions listed in the first and second columns of Table 2 in the shortest possible time. The number of variables and function constraints are provided in the fourth and fifth

columns, establishing upper and lower bounds for the function variables. The two-dimensional representations of these functions can be seen in Fig.7 and Fig. 8.

The evaluation of computational algorithms is typically gauged using two criteria: 1- The accuracy of the final solution 2- The computational speed. In this section, following the determination of these criteria for the aforementioned functions, the performance of ERO will be compared with Gray Wolf Optimization (GWO), Gravitational Search Algorithm (GSA), Particle Swarm Optimization (PSO), and Firefly Algorithm (FA).

The Gray Wolf Optimizer (GWO), introduced in 2014, is a novel meta-heuristic inspired by the hunting behavior of gray wolves. This algorithm emulates the hierarchical structure of gray wolf packs, utilizing four distinct types of wolves - alpha, beta, delta, and omega - in its simulation. The process involves three primary hunting stages: searching for prey, surrounding the prey, and ultimately attacking the prey [47].

Table 2. The 23 Benchmark Functions used in experimental study [77]

Name Function	Function	n	Range
Sphere Model	$F_1(x)=\sum_{i=1}^{n} x_i^2$	30	[-100,100]
Schwefel's problem 2.22	$F_2(x)==\sum_{i=1}^{n}\|x_i\|+\prod_{i=1}^{n}\|x_i\|$	30	[-10,10]
Schwefel's problem 1.2	$F_3(x)=\sum_{i=1}^{n}(\sum_{j=1}^{i} x_j)$	30	[-100,100]
Schwefel's problem 2.21	$F_4(x)=\max_i\{\|x_i\|, 1\le i\le n\}$	30	[-100,100]
Generalized Rosenbrock's function	$F_5(x)=\sum_{i=1}^{n-1}[100(x_{i+1}-x_i^2)^2+(x_i-1)^2]$	30	[-30,30]
Step function	$F_6(x)=\sum_{i=1}^{n}[x_i+0.5]^2$	30	[-100,100]
Quartic function with noise	$F_7(x)=\sum_{i=1}^{n} ix_i^4+random([0,1])$	30	[-1.28,1.28]
Generalized Schwefel's problem 2.26	$F_8(x)=\sum_{i=1}^{n} -x_i\sin(\sqrt{\|x_i\|})$	30	[-500,500]
Generalized Rastrigin's Function	$F_9(x)=\sum_{i=1}^{n}\left(x_i^2-10\cos\cos(2\pi x_i)+10\right)$	30	[-5.12,5.12]

Ackley's function	$f_{10}(x) = -20\exp(-0.2\sqrt{\frac{1}{n}\sum_{i=1}^{n} x_i^2}) - \exp(\frac{1}{n}\sum_{i=1}^{n}\cos(2\pi x_i)) + 20 + e$	30	[-32,32]

Table 2. The 23 Benchmark Functions used in experimental study [77] (continues)

Name Function	Function	n	Range
Generalized Griewank Function	$F_{11}(x) = \frac{1}{4000}\sum_{i=1}^{n} x_i^2 - \prod_{i=1}^{n}\cos\cos\left(\frac{x_i}{\sqrt{i}}\right) + 1$	30	[-600,600]
Generalized Penalized Functions	$F_{12}(x) = \frac{\pi}{n} \times \{10\sin^2(\pi y_1) + \sum_{i=1}^{n-1}(y_i - 1)^2(1 + 10\sin^2(\pi y_{i+1}) + (y_n - 1)\ \} + \sum_{i=1}^{n} u(x_i, 10, 100, 4)$ $y_i = 1 + \frac{1}{4}(x_i + 1)$ $u(x_i, a, k, m) = \begin{cases} k(x_i - a)^m & x_i \succ a \\ 0 & -a \le x_i \le a \\ k(-x_i - a)^m & x_i \prec -a \end{cases}$	30	[-50,50]
Generalized Penalized Functions	$F_{13}(x) = 0.1\{\ \sin^2(3\pi x_1) + \sum_{i=1}^{n-1}(x_i - 1)^2(1 + \sin^2(3\pi x_{i+1}) + (x_n - 1)^2(1 + \sin^2(2\pi x_n))\ \} + \sum_{i=1}^{n} u(x_i, 5, 100, 4)$ $u(x_i, a, k, m) = \begin{cases} k(x_i - a)^m & x_i > a \\ 0 & -a \le x_i \le a \\ k(-x_i - a)^m & x_i < -a \end{cases}$	30	[-50,50]
Shekel's Foxholes function	$F_{14}(x) = [\frac{1}{500} + \sum_{j=1}^{25}\frac{1}{j + \sum_{i=1}^{2}(x_i - \alpha_{ij})^6}]^{-1}$	2	[-65.536,65.536]
Kowalik's function	$F_{15}(x) = \sum_{i=1}^{11}[a_i - \frac{x_1(b_i^2 + b_i x_2)}{b_i^2 + b_i x_3 + x_4}]^2$	4	[-5,5]

Six-hump camel back function	$F_{16}(x) = 4x_1^2 - 2.1x_1^4 + \frac{1}{3}x_1^6 + x_1x_2 - 4x_2^2 + 4x_2^4$	4	[-5,5]

Table 2. The 23 Benchmark Functions used in experimental study [77] (continues)

Name Function	Function	n	Range
Branin function	$F_{17}(x) = (x_2 - \frac{5.1}{4\pi^2}x_1^2 + \frac{5}{\pi}x_1 - 6)^2 + 10(1 - \frac{1}{8\pi})\cos x_1 + 10$	2	[-5,5]×[0,10]
Goldstein-Price function	$F_{18}(x) = [1 + (x_1 + x_2 + 1)^2(19 - 14x_1 + 3x_1^2 - 14x_2 + 6x_1x_2 + 3x_2^2)] \times [30 + (2x_1 - 3x_2)^2(18 - 32x_1 + 12x_1^2 + 48x^2 - 36x_1x_2 + 27x_2^2)]$	2	[-2,2]
Hartman's family	$F_{19}(x) = -\sum_{i=1}^{4} c_i \exp[-\sum_{j=1}^{3} a_{ij}(x_j - p_{ij})^2]$	3	[0,1]
Hartman's family	$F_{20}(x) = -\sum_{i=1}^{4} c_i \exp[-\sum_{j=1}^{6} a_{ij}(x_j - p_{ij})^2]$	6	[0,1]
Shekel's family	$F_{21}(x) = -\sum_{i=1}^{5} [(x - a_i)(x - a_i)^T + c_i]^{-1}$	4	[0,10]
Shekel's family	$F_{22}(x) = -\sum_{i=1}^{7} [(x - a_i)(x - a_i)^T + c_i]^{-1}$	4	[0,10]
Shekel's family	$F_{23}(x) = -\sum_{i=1}^{10} [(x - a_i)(x - a_i)^T + c_i]^{-1}$	4	[0,10]

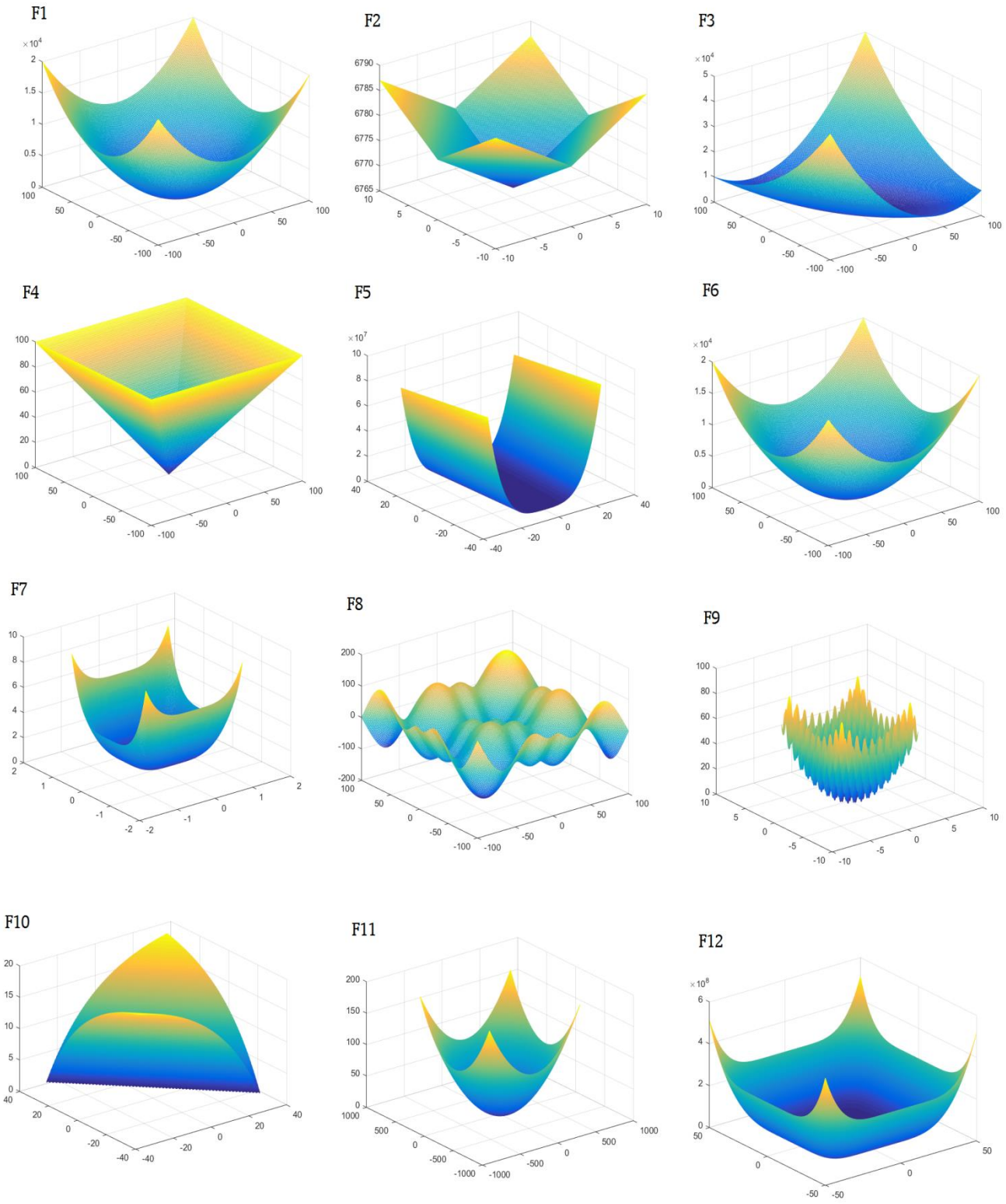


Fig. 7. Graphs of functions (F1-F12) for n=2

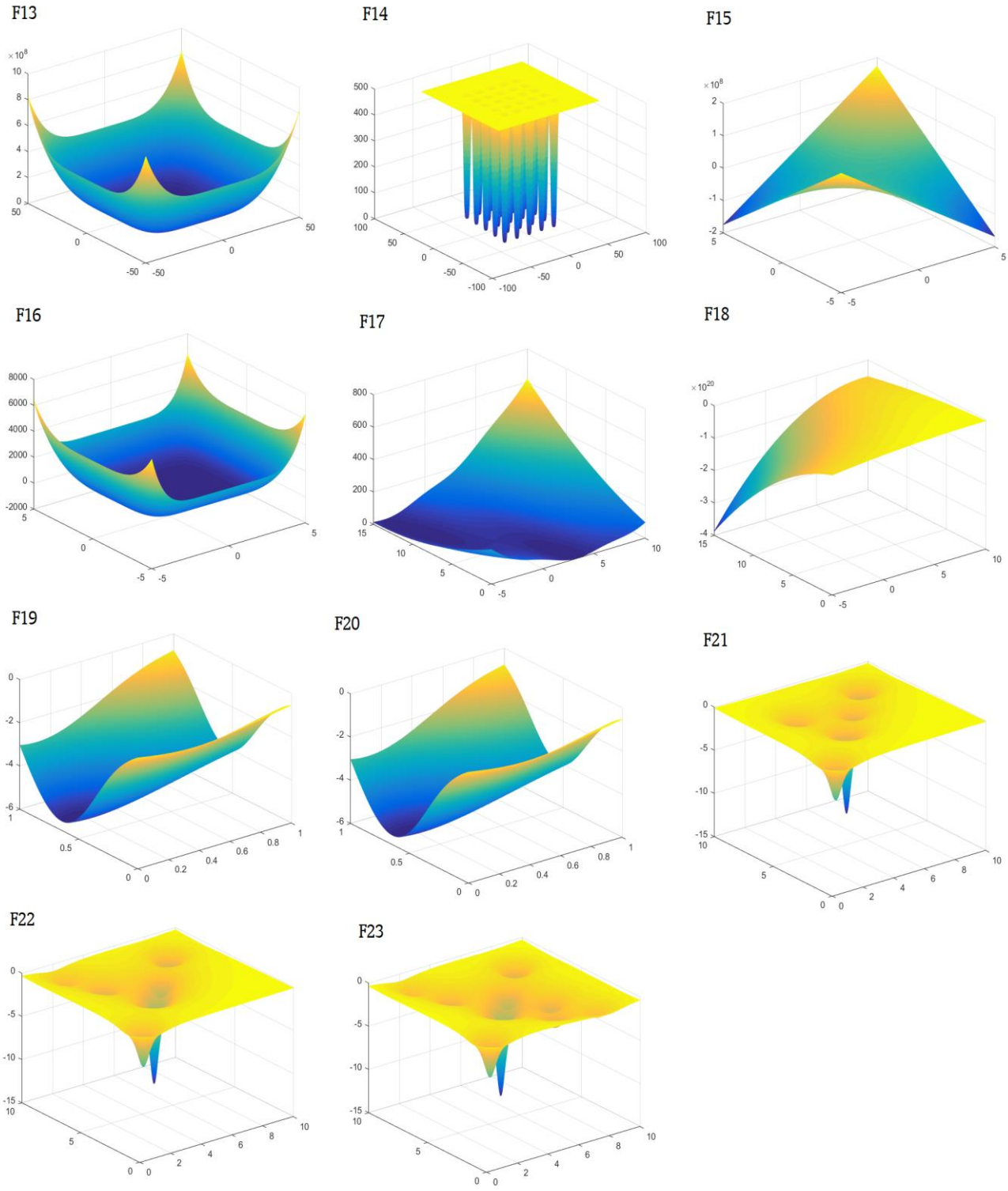


Fig. 8. Graphs of functions (F13- F23) for n=2

Another algorithm discussed in this paper is the Gravitational Search Algorithm (GSA), which operates based on physical laws such as gravity. In GSA, a collection of masses follows rules of movement that affect each other and lead to an improved final optimal answer. GSA was developed in 2009 [78].

The Firefly Algorithm (FA) was introduced by Xinshe Yang, a scholar from Cambridge, in 2008 [79]. FA is a random search algorithm inspired by swarm intelligence, simulating the attraction mechanism between individual fireflies in nature [80].

In 1995, an algorithm based on the intelligent collective behavior of animals in nature was discovered for stochastic optimization. This algorithm, called Particle Swarm Optimization (PSO), has seen advanced versions published. Numerous studies have been conducted and published regarding the effects of its parameters [81].

Table 3 presents the simulation results of the algorithm introduced in this paper (ERO) and compares it with PSO, GSA, FA, and GWO. The results include the mean run time and mean fitness of the best values found in 30 independent runs with separate seeds. The best accuracy of the algorithms is highlighted in green in Table 3, while yellow indicates that ERO is the second-most accurate.

Table 3. The average of final best fitness and the mean running time for 30 runs of minimizing benchmark functions, number of iterations=100

Algorithm		PSO	GSA	FA	GWO	ERO
$F_1(x)$	Mean Fitness	2.75	59137	0.26	1.61×10^{-5}	6.23×10^{-6}
	Mean Time	3.29	11.89	17.6	0.65	0.086
$F_2(x)$	Mean Fitness	0.55	2.22	2.37	6.92×10^{-4}	0.01
	Mean Time	3.73	12.43	15.72	0.79	0.09
$F_3(x)$	Mean Fitness	1035	99701	1278	17.85	4.6×10^{-3}
	Mean Time	3.27	21.8	13.37	0.64	0.089
$F_4(x)$	Mean Fitness	4.75	82.65	6.25	0.19	3.07×10^{-4}
	Mean Time	3.56	14.63	13.16	0.44	0.09
$F_5(x)$	Mean Fitness	252	3.85×10^{7}	294	28.23	9.2×10^{-3}
	Mean Time	3.4	13.42	13.37	0.49	0.09
$F_6(x)$	Mean Fitness	6.67	5.96×10^{4}	0.87	0.03	0
	Mean Time	3.49	23.9	11.74	0.63	0.087
$F_7(x)$	Mean Fitness	0.029	0.27	0.046	0.005	0.0098
	Mean Time	2.97	22.9	14.09	0.77	0.10
$F_8(x)$	Mean Fitness	-67993	-2546	-2705	-6003	-10727
	Mean Time	2.96	13.97	12.85	0.87	0.01
$F_9(x)$	Mean Fitness	37.54	62	97	21.16	0.0027
	Mean Time	2.91	21.63	12.21	0.6548	0.09
$F_{10}(x)$	Mean Fitness	1.42	19	0.91	0.001	0.0014
	Mean Time	3.03	24.83	6.43	1.138	0.1
$F_{11}(x)$	Mean Fitness	0.97	563	0.21	0.018	5.8×10^{-7}
	Mean Time	3.43	24.9	11.26	0.5157	0.09
$F_{12}(x)$	Mean Fitness	0.54	2.52×10^{8}	0.29	0.071	3.08×10^{-7}
	Mean Time	4.49	22.82	13.5	1.912	0.14
$F_{13}(x)$	Mean Fitness	0.5	4.91×10^{8}	1.17	0.79	2.6×10^{-7}
	Mean Time	4.88	18.91	12.55	1.69	0.13
$F_{14}(x)$	Mean Fitness	1.75	1.77	3.91	2.18	6.14
	Mean Time	3.88	6.62	12.73	0.72	0.11
$F_{15}(x)$	Mean Fitness	0.001	0.001	0.001	0.0032	7.3×10^{-7}
	Mean Time	0.99	15.99	12.49	0.4846	0.09
$F_{16}(x)$	Mean Fitness	-1.03	-1.03	-1.03	-1.03	-1.00
	Mean Time	3.45	15.2	5.89	0.33	0.08
$F_{17}(x)$	Mean Fitness	0.4	0.4	0.4	0.4	2.29
	Mean Time	3.44	12.58	13.25	0.37	0.08
$F_{18}(x)$	Mean Fitness	-592103	-576415	-592103	-529210	-591830
	Mean Time	3.96	13.92	12.29	0.3452	0.08
$F_{19}(x)$	Mean Fitness	-3.89	-3.85	-3.86	-3.86	-3.67
	Mean Time	3.35	14.68	12.06	0.45	0.09
$F_{20}(x)$	Mean Fitness	-3.27	-3.03	-3.22	-3.23	-2.40
	Mean Time	4.02	15.28	13.22	0.53	0.09
$F_{21}(x)$	Mean Fitness	-6.97	-6.24	-7.81	-9.54	-9.86
	Mean Time	5.05	14.31	12.72	0.97	0.13
$F_{22}(x)$	Mean Fitness	-7.88	-8.82	-10.14	-10.12	-10.37
	Mean Time	5.24	14.39	13.9	1.21	0.13
$F_{23}(x)$	Mean Fitness	-6.6	-8.82	-10.53	-10.24	-10.45
	Mean Time	5.57	17.1	14.37	1.68	0.14

To obtain the performance rating for these 5 algorithms (ERO, PSO, GSA, FA and GWO), the Eq. (7) is suggested:

✉**Mahdi Tourani**
tourani.mahdi@birjand.ac.ir

$$Mean\ R = \frac{\sum_{i=1}^{5} (\#\text{Rank}\, i) \times i}{\sum_{i=1}^{5} i} \quad (7)$$

where *Mean R* indicates the average weighted rank and *#Rank i* represents the number of rank i in all test functions. Tables 4 and 5 display the results of the number of ranks for each algorithm across all test functions, as well as the final rank among the algorithms based on Eq. (7). In these tables, *#Ri* denotes the number of rank i in all test functions. The green color in Tables 4 and 5 highlights the best performance of the algorithms.

Table 4. The results of the number of accuracy ranks for each algorithm in the all test functions and the final rank among the algorithms

	#R1	#R2	#R3	#R4	#R5	Mean R	Final Rank
ERO	15	2	1	0	5	2.93	1
GWO	1	14	5	1	2	3.86	2
PSO	6	3	6	6	2	4.27	3
FA	1	3	10	7	2	5	4
GSA	0	1	1	9	12	6.73	5

Table 5. The results of the number of running time ranks for each algorithm in the all test functions and the final rank among the algorithms

	#R1	#R2	#R3	#R4	#R5	Mean R	Final Rank
ERO	23	0	0	0	0	1.53	1
GWO	0	23	0	0	0	3.06	2
PSO	0	0	23	0	0	4.6	3
GSA	0	0	19	4	0	4.86	4
FA	0	0	4	19	0	5.86	5

When comparing algorithms to determine the best performance, both speed and accuracy should be considered together. Therefore, based on the results, it is evident that Elymus Repens Optimization (ERO) demonstrates the best overall performance in terms of accuracy and speed indexes.

6- Conclusions and Future Work

Optimization is one of the most important processes in the industry. Among the various methods, meta-heuristic algorithms are the most powerful for optimization. This paper introduces a new algorithm called Elymus Repens Optimization (ERO) based on the behavior of Elymus Repens in agricultural land. The effectiveness and power of ERO are then evaluated using 23 well-known benchmark functions to demonstrate its capabilities. Following this simulation, the performance of ERO is compared with other optimization algorithms such as Gray Wolf Optimization (GWO), Firefly Algorithm (FA), Particle Swarm Optimization (PSO), and Gravitational Search Algorithm (GSA). Results indicate that the proposed algorithm is highly efficient in terms of accuracy and speed.

Based on the desirable result of the algorithm, presented in this paper (ERO), it is recommended that this be implemented for optimization problems in the industry.

References

[1]. S.A. Mirjalili, "The Ant Lion Optimizer", Advances in Engineering Software , Vol. 83 , pp. 80–98, 2015.

[2]. F. MiarNaeimi, G.R. Azizyan, M. Rashki, "Horse herd optimization algorithm: A nature-inspired algorithm for high-dimensional optimization problems", Knowledge-Based Systems, Vol. 213, pp. 1-17, 2021.

[3]. J.H. Holland, Adaptation in Natural and Artificial Systems: An Introductory Analysis with Applications to Biology, Control, and Artificial Intelligence, MIT press, 1992.

[4]. J.R. Koza, Genetic Programming: On the Programming of Computers By Means of Natural Selection, MIT press, 1992.

[5]. F. Glover, "Tabu search—Part I" , ORSA J. Comput. Vol. 1, No. 3, pp.190–206, 1989.

[6]. I. Rechenberg, J.M. Zurada, R.J. Marks II, C. Goldberg, Evolution strategy, in computational intelligence: Imitating life, in: Computational Intelligence Imitating Life, IEEE Press, Piscataway, 1994.

[7]. N.J. Radcliffe, P.D. Surry, "Formal Memetic Algorithms", in: AISB Workshop on Evolutionary Computing, Springer, pp. 1–16, 1994.

[8]. R.G. Reynolds, "An introduction to cultural algorithms", in: Proceedings of the Third Annual Conference on Evolutionary Programming, World Scientific, pp. 131–139,1994.

[9]. S. Kirkpatrick, C.D. Gelatt, M.P. Vecchi, "Optimization by simulated annealing", Science, Vol. 220 , No. 4598, pp. 671–680, 1983.

[10]. R. Storn, K. Price, "Differential evolution–a simple and efficient heuristic for global optimization over continuous spaces", J. Global Optim. Vol. 11, No.4, pp. 341–359, 1997.

[11]. X. Yao, Y. Liu, G. Lin, "Evolutionary programming made faster", IEEE Trans. Evol. Comput. Vol. 3 , No. 2, pp. 82–102, 1999.

[12]. Y.K. Kim, J.Y. Kim, Y. Kim, "A coevolutionary algorithm for balancing and sequencing in mixed model assembly lines", Appl. Intell. Vol. 13 , No. 3, pp. 247–258, 2000.

[13]. A. Sinha, D.E. Goldberg, "A Survey of Hybrid Genetic and Evolutionary Algorithms", IlliGAL report, Vol. 2003004, 2003.

[14]. E. Atashpaz-Gargari, C. Lucas, "Imperialist competitive algorithm: An algorithm for optimization inspired by imperialistic competition", in: 2007 IEEE Congress on Evolutionary Computation, IEEE, pp. 4661–4667, 2007.

[15]. D. Simon, "Biogeography-based optimization", IEEE Trans. Evol. Comput. Vol. 12 , No. 6, pp. 702–713, 2008.

[16]. E. Cuevas, A. Echavarría, M.A. Ramírez-Ortegón, "An optimization algorithm inspired by the states of matter

that improves the balance between exploration and exploitation", Appl. Intell. Vol. 40, No. 2 , pp. 256–272, 2014.
[17]. S. Mirjalili, "SCA: A sine cosine algorithm for solving optimization problems", Knowl.-Based Syst., Vol. 96, pp. 120–133, 2016.
[18]. F. MiarNaeimi, G. Azizyan, M. Rashki, "Multi-level cross entropy optimizer (MCEO): An evolutionary optimization algorithm for engineering problems", Eng. Comput., Vol. 34 , No. 4, 2018.
[19]. H. Du, X. Wu, J. Zhuang, "Small-world optimization algorithm for function optimization", in: International Conference on Natural Computation, Springer, pp. 264–273, 2006.
[20]. R.A. Formato, "Central force optimization: A new metaheuristic with applications in applied electromagnetics", in: Progress in Electromagnetics Research, PIER 77, pp. 425–491,2007.
[21]. M.H. Tayarani-N, M.R. Akbarzadeh-T, "Magnetic optimization algorithms a new synthesis", in: 2008 IEEE Congress on Evolutionary Computation (IEEE World Congress on Computational Intelligence), pp. 2659–2664, 2008.
[22]. E. Rashedi, H. Nezamabadi-Pour, S. Saryazdi, "GSA: A gravitational search algorithm", Inf. Sci., Vol. 179, No. 13, pp. 2232–2248, 2009.
[23]. A. Kaveh, S. Talatahari, "A novel heuristic optimization method: Charged system search", Acta Mech. Vol. 213, pp. 267–289, 2010.
[24]. A.Y.S. Lam, V.O.K. Li, "Chemical-reaction-inspired metaheuristic for optimization", IEEE Trans. Evol. Comput., Vol. 14, No 3, pp. 381–399, 2010.
[25]. A. Hatamlou, "Black hole: A new heuristic optimization approach for data clustering", Inf. Sci., Vol. 222 , pp. 175–184, 2013.
[26]. F.F. Moghaddam, R.F. Moghaddam, M. Cheriet, "Curved space optimization: A random search based on general relativity theory", arXiv, Vol. 1208, No. 2214, 2012.
[27]. A. Kaveh, T. Bakhshpoori, "Water evaporation optimization: A novel physically inspired optimization algorithm", Comput. Struct., Vol. 167, pp. 69–85, 2016.
[28]. H. Varaee, M.R. Ghasemi, "Engineering optimization based on ideal gas molecular movement algorithm", Eng. Comput. Vol. 33 , No. 1, pp. 71–93, 2017.
[29]. S. Mirjalili, S.M. Mirjalili, A. Hatamlou, "Multi-verse optimizer: A natureinspired algorithm for global optimization", Neural Comput. Appl., Vol. 27 , No. 2, pp. 495–513, 2016.
[30]. A. Kaveh, M.I. Ghazaan, "A new meta-heuristic algorithm: Vibrating particles system", Sci. Iran. Trans. A Civ. Eng., Vol. 24, No 2, pp. 551-566, 2017.
[31]. R. Eberhart, J. Kennedy, "A new optimizer using particle swarm theory", in: MHS'95. Proceedings of the Sixth International Symposium on Micro Machine and Human Science, IEEE, pp. 39–43, 1995.
[32]. S. Saremi, S. Mirjalili, A. Lewis, "Grasshopper optimisation algorithm: Theory and application", Adv. Eng. Softw., Vol. 105, pp. 30–47, 2017.
[33]. S. Mirjalili, "Moth-flame optimization algorithm: A novel nature-inspired heuristic paradigm", Knowl.-Based Syst., Vol. 89, pp.228–249, 2015.
[34]. X.L. Li, "A New Intelligent Optimization-Artificial Fish Swarm Algorithm", (Doctor thesis), Zhejiang University of Zhejiang, China, 2003.
[35]. D. Karaboga, "An Idea Based on Honey Bee Swarm for Numerical Optimization", Technical report-tr06, Erciyes university, engineering faculty, computer., 2005.
[36]. M. Roth, "Termite: A swarm intelligent routing algorithm for mobile wireless ad-hoc networks", Presented to the Faculty of the Graduate School of Cornell University in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy, 2005.
[37]. M. Dorigo, M. Birattari, T. Stutzle, "Ant colony optimization", IEEE Comput. Intell. Mag. Vol. 1, No. 4, pp. 28–39, 2006.
[38]. M. Eusuff, K. Lansey, F. Pasha, "Shuffled frog-leaping algorithm: A memetic meta-heuristic for discrete optimization", Eng. Optim., Vol. 38, No. 2, pp. 129–154, 2006.
[39]. A. Mucherino, O. Seref, "Monkey search: A novel metaheuristic search for global optimization", in: AIP Conference Proceedings, American Institute of Physics, pp. 162–173, 2007.
[40]. Y. Shiqin, J. Jianjun, Y. Guangxing, "A dolphin partner optimization", in: Intelligent Systems, GCIS'09. WRI Global Congress On, IEEE, pp. 124–128, 2009.
[41]. X.S. Yang, "Firefly algorithm, stochastic test functions and design optimisation", arXiv, Vol. 1003, No. 1409, 2010.
[42]. X.S. Yang, "A new metaheuristic bat-inspired algorithm", in: Nature Inspired Cooperative Strategies for Optimization (NICSO 2010), Springer, pp. 65–74, 2010.
[43]. A. Askarzadeh, A. Rezazadeh, "A new heuristic optimization algorithm for modeling of proton exchange membrane fuel cell: Bird mating optimizer", Int. J. Energy Res., Vol. 37, No. 10, pp.1196–1204, 2013.
[44]. W.T. Pan, "A new fruit fly optimization algorithm: Taking the financial distress model as an example", Knowl.-Based Syst., Vol. 26, pp. 69–74, 2012.
[45]. B. Wang, X. Jin, B. Cheng, "Lion pride optimizer: An optimization algorithm inspired by lion pride behavior", Sci. China Inf. Sci., Vol. 55, No. 10, pp. 2369–2389, 2012.
[46]. A.H. Gandomi, A.H. Alavi, "Krill herd: A new bio-inspired optimization algorithm", Commun. Nonlinear Sci., Vol. 17 , No. 12, pp. 4831–4845, 2012.
[47]. S. Mirjalili, S.M. Mirjalili, A. Lewis, "Grey wolf optimizer", Adv. Eng. Softw., Vol. 69 , pp. 46–61, 2014.
[48]. A.H. Gandomi, X.S. Yang, A.H. Alavi, "Cuckoo search algorithm: A metaheuristic approach to solve structural optimization problems", Eng. Comput., Vol. 29, No. 1, pp. 17–35, 2013.
[49]. S. Mirjalili, "Dragonfly algorithm: A new meta-heuristic optimization technique for solving single-objective, discrete, and multi-objective problems", Neural Comput. Appl., Vol. 27, No. 4 , pp. 1053–1073, 2016.
[50]. S. Mirjalili, "A. Lewis, The whale optimization algorithm", Adv. Eng. Softw., Vol. 95, pp. 51–67, 2016.
[51]. S. Mirjalili, A.H. Gandomi, S.Z. Mirjalili, S. Saremi, H. Faris, S.M. Mirjalili, "Salp swarm algorithm: A bio-inspired optimizer for engineering design problems", Adv. Eng. Softw., Vol. 114, pp.163–191, 2017.

[52]. A.A. Heidari, S. Mirjalili, H. Faris, I. Aljarah, M. Mafarja, H. Chen, "Harris hawks optimization: Algorithm and applications", Future Gener. Comput. Syst., Vol. 97 pp. 849–872, 2019.

[53]. G. Azizyan, F. Miarnaeimi, M. Rashki, N. Shabakhty, "Flying squirrel optimizer (FSO): A novel SI-based optimization algorithm for engineering problems", Iran. J. Optim., Vol. 11, No. 2, pp.177–205, 2019.

[54]. N. Moosavian, B.K. Roodsari, "Soccer league competition algorithm: A novel meta-heuristic algorithm for optimal design of water distribution networks", Swarm Evol. Comput., Vol. 17, pp. 14–24, 2014.

[55]. A.A. Volk, R.W. Epps, D.T. Yonemoto, S. B.Masters, F. N. Castellano, K. G. Reyes , M. Abolhasani.,"AlphaFlow: autonomous discovery and optimization of multi-step chemistry using a self-driven fluidic lab guided by reinforcement learning",Nat Commun, Vol. 14, 2023.

[56]. A.M.K. Nambiar, C. P. Breen,T. Hart, T. Kulesza, T. F. Jamison, K. F. Jensen". Bayesian optimization of computer-proposed multistep synthetic routes on an automated robotic flow platform", ACS Cent. Sci. Vol. 8,pp. 825–836, 2022

[57]. Y. Jiang, D. Salley, A. Sharma, G. Keenan, M. Mullin -, L. Cronin," An artificial intelligence enabled chemical synthesis robot for exploration and optimization of nanomaterials", Sci. Adv. , Vol. 8, 2022.

[58]. D. Karan, G. Chen, N. Jose, J. Bai, P. McDaid, A.A. Lapkin, " A machine learning-enabled process optimization of ultra-fast flow chemistry with multiple reaction metrics", Reaction Chemistry & Engineering, vol. 9, pp. 619-629, 2024.

[59]. G.-N. Ahn, J.H. Kang, H.J. Lee, B.E. Park, M. Kwon, G.S. Na, H. Kim, D.H. Seo, D.P. Kim., "Exploring ultrafast flow chemistry by autonomous self-optimizing platform", Chem. Eng. J., Vol. 453, 2023.

[60]. M. Gholami, S.M. Muyeen, S. Lin,"Optimizing microgrid efficiency: Coordinating commercial and residential demand patterns with shared battery energy storage,Journal of Energy Storage,Volume 88,2024.

[61]. D. Borkowski, P. Oramus, M. Brzezinka, "Battery energy storage system for grid-connected photovoltaic farm – energy management strategy and sizing optimization algorithm", J. Energy Storage, Vol. 72 , 2023

[62]. K. Ullah, J. Quanyuan, G. Geng, R.A. Khan, S. Aslam, W . Khan," Optimization of demand response and power-sharing in microgrids for cost and power losses", Energies, Vol. 15, 2022.

[63]. S. Sakina Zaidi, S.S. Haider Zaidi, B.M. Khan, L. Moin,"Optimal designing of grid-connected microgrid systems for residential and commercial applications in Pakistan", Heliyon, Vol. 9 , 2023.

[64]. R. Asri, H. Aki, D. Kodaira," Optimal operation of shared energy storage on islanded microgrid for remote communities", Sustain. Energy, Grids Networks,Vol. 35 , 2023.

[65]. Q. Huang, H. Ding, N. Razmjooy, "Oral cancer detection using convolutional neural network optimized by combined seagull optimization algorithm", Biomedical Signal Processing and Control, Vol. 87, Part B, 2024.

[66]. M. M. Emam, E. H. Houssein, N. A.Samee, M. A. Alohali, M. E. Hosney, " Breast cancer diagnosis using optimized deep convolutional neural network based on transfer learning technique and improved Coati optimization algorithm", Expert Systems with Applications, Vol. 255, Part B,2024.

[67]. S. Almutairi, S. Manimurugan, B. G. Kim, M.M. Aborokbah, C. Narmatha, "Breast cancer classification using Deep Q Learning (DQL) and gorilla troops optimization (GTO)", Applied Soft Computing, Vol. 142, 2023

[68]. M. M. Emam, N. A. Samee, M. M. Jamjoom, E. H. Houssein, "Optimized deep learning architecture for brain tumor classification using improved Hunger Games Search Algorithm", Computers in Biology and Medicine, Vol. 160, 2023.

[69]. W. Zou, X. Luo, M. Gao, C. Yu, X. Wan, S. Yu, Y. Wu, A. Wang, W. Fenical, Z. Wei, Y. Zhao, Y. Lu, " Optimization of cancer immunotherapy on the basis of programmed death ligand-1 distribution and function", Vol. 181 , Themed Issue: Cancer Microenvironment and Pharmacological Interventions, pp. 257-272, 2024.

[70]. J. Palmer, G. Sagar, "Agropyron repens (L.) Beauv. (Triticum repens L.; Elytrigia repens (L.) Nevski)", J. Ecol., Vol. 51, pp. 783–794, 1963.

[71]. P.A. Werner, R. Rioux, "The biology of Canadian weeds. 24. Agropyron repens (L.) Beauv. Can." J. Plant Sci., Vol. 57, pp. 905–919, 1977.

[72]. L.G. Holm, D.L. Plucknett., J.V. Pancho, J.P. Herberger, The World's Worst Weeds, University Press: Honolulu, HI, USA, 1977.

[73]. C. Andreasen, I.M. Skovgaard, "Crop and soil factors of importance for the distribution of plant species on arable fields in Denmark", Agric. Ecosyst. Environ., Vol. 133, pp. 61–67, 2009.

[74]. J. Salonen, T. Hyvönen, H.A. Jalli, "Composition of weed flora in spring cereals in Finland—A fourth survey", Agric. Food Sci., Vol. 20, 2011.

[75]. P. A. Werneri , R. Rioux, "The Biology of Canadian Weeds. 24. Agropyron Repens (L.) Beauv", Canadian Journal of Plant Science, Vol. 57, pp. 905-919.

[76]. K.M. Ibrahim, P.M. Peterson, Grasses of Washington, D.C., Published by Smithsonian Institution Scholarly Press, Washington D.C., 2014.

[77]. X. Yao, Y. Liu, G. Lin, "Evolutionary Programming Made Faster", IEEE Transactions on Evolutionary Computation, Vol. 3, No. 2, pp. 82-102, 1999.

[78]. E. Rashedi, H. Nezamabadi-pour, S. Saryazdi, " GSA: A Gravitational Search Algorithm", Information Sciences, Vol. 179, pp. 2232–2248, 2009.

[79]. X. Yang, " Firefly algorithms for multimodal optimization", International conference on stochastic algorithms foundations and applications, pp.169–178, 2009.

[80]. Y. Li, Y. Zhao, Y. Shang, J. Liu " An improved firefly algorithm with dynamic self-adaptive adjustment", PLoS ONE, Vol. 16 ,2021.

[81]. D. Wang, D. Tan, L. Liu, " Particle swarm optimization algorithm: an overview", Soft Comput., Vol. 22, pp. 387–408 , 2018.

Journal of Information Systems and Telecommunication
Vol.12, No.3, July-September 2024, 208-219
http://jist.acecr.org
ISSN 2322-1437 / EISSN:2345-2773

Improving Opinion Mining Through Automatic Prompt Construction

Arash Yousefi Jordehi[1], Mahsa Hosseini Khasheh Heyran[1], Saeed Ahmadnia[1], Seyed Abolghasem Mirroshandel[1*], Owen Rambow[2]

[1].Department of Computer Engineering, Faculty of Engineering, University of Guilan, Rasht, Guilan, Iran
[2].Department of Linguistics, Stony Brook University, Stony Brook, NY, USA

Received: 20 Apr 2024/ Revised: 14 Sep 2024/ Accepted: 30 Sep 2024

Abstract

Opinion mining is a fundamental task in natural language processing. This paper focuses on extracting opinion structures: triplets representing an opinion, a part of text involving an opinion role, and a relation between opinion and role. We utilize the T5 generative transformer for this purpose. It also adopts a multi-task learning approach inspired by successful previous studies to enhance performance. Nevertheless, the success of generative models heavily relies on the prompts provided in the input, as prompts customize the task at hand. To eliminate the need for human-based prompt design and improve performance, we propose Automatic Prompt Construction, which involves fine-tuning. Our proposed method is fully compatible with multi-task learning, as we did so in our investigations. We run a comprehensive set of experiments on Multi-Perspective Question Answering (MPQA) 2.0, a commonly utilized benchmark dataset in this domain. We observe a considerable performance boost by combining automatic prompt construction with multi-task learning. Besides, we develop a new method that re-uses a model from one problem setting to improve another model in another setting as a Transfer Learning application. Our results on the MPQA represent a new state-of-the-art and provide clear directions for future work.

Keywords: Opinion Mining/Sentiment Analysis; Statistical and Machine Learning Methods; Large Language Models; MPQA; Automatic Prompt Construction.

1- Introduction

Extracting opinion entities, such as opinion expressions, opinion holders, and opinion targets is one of the most interesting problems in Opinion Mining (OM), which clarifies *Who expressed or experienced what type of cognitive state toward which entity?* [1, 2, 3, 4]. A cognitive state can be defined as the state of a source (holder or experiencer of the cognitive state, also known as the agent) holding an attitude (via an opinionated expression within the text) toward a target [5, 6]. In this paper, we refer to the opinion expression as the expression, the opinion holder as the agent, and the opinion target as the target. We refer to the (expression, role, relation) triplet as an opinion structure. In fine-grained OM, an expression might be coupled with one or more roles (agents and/or targets). An expression may also not have any agent or target [7, 4]. In this paper, we focus on detecting expressions, agents, and targets, and the structures they form. Similar to much previous research [8, 2, 3, 1], we have focused on a subset of the Multi-Perspective Question Answering (MPQA) 2.0 dataset in our paper. This subset is frequently used as a benchmark dataset in research focused on detecting opinion expressions and identifying their roles, such as agent and target. The MPQA Corpus contains news articles and other text documents manually annotated for opinions and other cognitive states. Examining prior work indicates that using the aforementioned dataset for fine-grained OM problems is a suitable choice, as most studies have relied solely on this dataset. In our perspective, MPQA is highly complex and has many aspects that remain unexplored. Mastering MPQA, of course, requires significant time. Previous work typically concentrated on using a tagging mechanism in order to label tokens and extract opinion expression and roles. However, the main drawback of using this approach is that it cannot capture cases where there is an overlap between opinion arguments (i.e., roles) of two different

✉ **Seyed Abolghasem Mirroshandel**
mirroshandel@guilan.ac.ir

opinion expressions, as one word can be assigned to only one tag. This approach does not adequately capture the essence of the problem. Xia et al. [3] proposed "SpanOM", in which a two-step algorithm is adopted: 1) Binary prediction on word span in order to detect that the word span is an expression or role or neither. 2) Allocation of opinion relations to the pairs of (expression, role). Their approach solves the issue of overlapping opinion roles mentioned earlier, but on the other hand it has a high computational complexity and lack of explicit interaction between expressions and roles. The most recent research [9], solved the problem by proposing a neural transition model which is highly affected by language knowledge provided to the system. We propose a generative system called Generative Opinion Mining, the "GenOM" system. GenOM avoids the weaknesses of some previous studies and mainly uses modern architectures. Recent studies have demonstrated the success of using transformers [10, 11, 3, 12, 13, 14, 15, 16], such as Text-to-Text Transfer Transformer (T5) [17], which improve the performance compared to traditional machine learning algorithms, manual feature engineering and also deep CNNs and RNNs. In our research, due to the successful results of T5, we aim to utilize it. Furthermore, our model is not dependent on any external natural language prerequisites. In the current study, we address two settings. First, we predict the (expression, role, relation) triplet directly from a sentence (i.e. end-to-end setting). Second, we include the expression in the input and predict its roles (i.e. agents and targets) (called given expression setting). These two settings are also used in a number of previous studies and our proposed GenOM system is capable of performing in both. The problem can be viewed as several related sub-tasks, namely detecting the expression, the agent, and the target from the sentence, and detecting the agent and the target from the sentence and the expression. Because we have distinct but related sub-tasks, we can apply Multi-task Learning (MTL) which strongly improves performance. Following the standard methodology for fine-tuning, we prepend to the sentence (or to the combination of sentence and expression in the given-expression setting) a prompt indicating the sub-task, which then prompts the model to generate that sub-task's output. It turns out that finding an efficient prompt for a given problem by hand and trial-and-error is very time-consuming and problem-dependent. Hence, we propose an approach for finding an efficient prompt automatically, Automatic Prompt Construction (APC). GenOM synthesizes each sub-task's output and uses these results to assemble the predicted triplet (end-to-end setting) or pair (given-expression setting). Then, we measure our system's performance by metrics used in the previous studies. Finally, by comparing our work to other research, we observe successful results of our proposed methods. We also show that using either MTL or APC strongly improves performance, compared to the simple use of transformers, and that these improvements are additive.

The main contributions of our paper lie in the following key points:

- Proposing a generative approach based on MTL to solve the OM problem consists of three main tasks: 1) Expression prediction, 2) Roles prediction through an end-to-end manner, and 3) Roles prediction employing the given-expression method, referred to as the Opinion Role Labeling (ORL) problem in prior literature.
- Suggesting and implementing the APC approach to improve the efficiency of generative prompt-based text-to-text models and obviate the requirement for manually crafted prompts. It offers a novel and efficient approach for optimizing prompts in today's widely used text-to-text language models. This approach could be used for any pre-trained large language model or transformer which accepts (or affected by) prefixes or prompts. It is worth mentioning that the T5 transformer has not been the only choice in the past years. Other text-to-text transformers such as BART [18] and FLAN-T5 [19] have been available since their presentation. However, we presume adopting models like T5 or BART was not successful in previous endeavors of other researchers as they are significantly dependent on input/output structure and prompts provided to them.
- Achieving state-of-the-art (SOTA) and near SOTA results in all benchmark tasks without using external sources of knowledge (e.g., parse tree information), and using only the base version (i.e., medium size in terms of parameters) of T5.

The remainder of this paper is arranged as follows. In section 2, we review previous work. Then, in Section 3, we explain our Generative Opinion Mining, the "GenOM", algorithm. Section 4 introduces the benchmark dataset, the experimental setup, and hyper-parameters with all essential details. In Section 5, after presenting our experimental results, we discuss our results. We also conducted a comprehensive comparison of our approaches with existing

successful algorithms. Finally, in Section 6, we conclude and outline the future work.

2- Related Work

Research in the OM field can be categorized into four groups. The first group consists of opinion expression extraction and labeling [20, 21, 22]. The second group is opinion structure recognition in an end-to-end fashion [23, 24, 25, 9]. The third group of research is Opinion Role Labeling (ORL), which includes the expression in the input (i.e. given-expression setting) as a means to detect its corresponding opinion roles [1, 8, 2]. Afterwards, Xia et al. [3] proposed a system to address OM in the most comprehensive way (i.e., including the end-to-end and given-expression tasks) and to overcome issues observed in the earlier works. As an illustration, inability to capture the semantic dependencies between words which are far apart is mentioned as one drawback of previous research.

Prior research frequently used BMESO-based tags to unravel the problem. BMESO-based tagging tags every token with one of the BMESO tags. B, M, and E tags encode the beginning, middle, and ending word of a role, and the S and O tags represent single-word roles and other words [8]. Therefore, techniques based on Conditional Random Fields (CRF) seemed to be a good choice [21]. Another study [23] recommended using a specific type of recurrent neural networks, called Bi-directional Long Short Term Memory (BiLSTM), in combination with CRF to construct the BiLSTM-CRF model. Their intention is to assign a label to each word in the sentence. Subsequently, they designate the relation to the expression with the set of two features: assigned label and distance to the expression. In other research [25], they designed an end-to-end transition-based system which actually determines the expressions and roles. In other words, they encode the input sentence by a multi-layer BiLSTM. Then, they detect opinion expressions and roles by using manually designed transition actions. Quan et al. [24] derived Bidirectional Encoder Representations from Transformers (BERT) [26] contextualized representations of sentences in order to synthesize BERT and BiLSTM-CRF. In consonance with what was mentioned, models based on sequence tagging are not able to detect opinion roles (agent/target) corresponding to distinct expressions in a sentence.

Table 1. Summary of Key Opinion Mining Studies, Methods, Models, and Identified Research Gaps.

Study	**Methodology**	**Utilized Model**	**Main Findings**	**Limitations**	**Research Gap Addressed by The Study**
Xia et al. [3]	Unified span-based approach with syntactic constituents	SpanOM	Improved detection of opinion expressions and roles using a span-based method.	High computational complexity, lack of explicit interaction between expressions and roles.	Overcomes complexity and enhances interaction through generative modeling.
Wu et al. [8]	Neural transition model joined with PointNet	Neural Transition Model	Successfully detects opinion structures in an end-to-end fashion.	Highly reliant on external syntactic knowledge, limited to end-to-end detection only.	Proposes a generative approach that does not depend on external syntactic knowledge.
Zhang et al. [7]	MTL with Semantic Role Labeling (SRL)	Semantic-aware BiLSTM-CRF	Enhances opinion role labeling by incorporating SRL outputs as inputs.	Depends heavily on SRL outputs, which may not always be available or reliable.	Uses automatic prompt construction without reliance on external knowledge.
Quan et al. [23]	End-to-end joint opinion role labeling with BERT	BiLSTM-CRF with BERT representations	Combines BERT with BiLSTM-CRF for improved contextual understanding.	Struggles with capturing complex opinion relationships and dependencies between	Employs a generative model capable of handling complex opinion structures directly.
Proposed Approach (This Study)	Generative framework using MTL and APC	T5 Transformer with MTL and APC	Achieves state-of-the-art performance, optimizes prompt construction automatically, and integrates end-to-end and given-expression settings for improved accuracy.	Does not rely on external syntactic or semantic knowledge, simplifies model training, and reduces manual prompt design efforts.	Introduces a novel generative approach combining MTL and APC, setting new benchmarks for opinion mining.

On the benchmark dataset, there is some research to adopt a variety of external knowledge to boost the performance. Marasović and Frank [1] used MTL with Semantic Role Labeling (SRL) to address the scarcity of data by leveraging the semantic knowledge. Another team of researchers [8] utilized the SRL outputs as inputs to the OM system which results in a significant boost in performance. In another study [11], they used the rich representations of BERT to be fed in a deep BiLSTM-CRF model. Xia et al. [3] suggested a new method instead of BMESO, that consists of three sub-tasks: 1) Opinion expression detection. 2) Opinion role detection. 3) Opinion relation detection. They perform these sub-tasks in the MTL fashion. In addition, they used syntactic constituents to enhance their performance. However, as noted by Wu et al. [9], it suffers from some issues. For instance, the computational complexity of their approach is very high (i.e., $\mathcal{O}(n^4)$), due to the necessity of processing all possible spans. Also, when their model tries to capture interplays between opinion expressions and roles explicitly, it ends in failure. Recently, Wu et al. [9] designed a complex system for detecting opinion structures only in the end-to-end way. Their system comprises a neural transition model joined with a PointNet [27] in order to accurately find the boundaries of opinion expressions and roles. Similar to some other past research efforts, they utilize external syntax knowledge to improve their system. More precisely, there is a requirement of dependency structure and part-of-speech tags for each input. In Table 1, we provide a concise overview of the studies discussed in this section. This table highlights the key methods, models, and findings of each work, along with the research gaps our proposed approach aims to address.

3- Proposed Method

3-1- Formal Task Definition

We adopt the task definition presented by Xia et al. [3]. Given an arbitrary sentence, say s as input, where $s = w_1, w_2, \dots, w_n$, the system tries to predict the gold-standard opinion triplets $\mathcal{Y} \subseteq \mathrm{E} \times \mathrm{O} \times \mathrm{R}$, where E is the set of opinion expressions defined mathematically as $\mathrm{E} = \{w_i, \dots, w_j \mid 1 \leq i \leq j \leq n\}$, O is the set of opinion roles defined as $\mathrm{O} = \{w_i, \dots, w_j \mid 1 \leq i \leq j \leq n\}$, and R is the set of opinion relations ($\{\text{agent}, \text{target}\}$). While Xia et al. [3] use indices to represent text spans, we take a generative approach and actually generate words. Our proposed method is two-step: we recognize expressions (we can generate expressions standalone because they are not dependent on opinion roles explicitly), and then we predict the opinion role-expression pairs separately. More specifically, we will define three sub-tasks: i) Predicting expressions, ii) Predicting agent-expression pairs, and iii) Predicting target-expression pairs. These tasks could be done separately but we do them jointly, and after the prediction, we form triplets by linking these three sub-tasks' outputs. See Section 3.6 for more details.

3-2- T5 for Conditional Generation

T5 [17] is an encoder-decoder transformer [28] which has been proposed to tackle problems in a generative manner supported by text-to-text learning. More precisely, we use T5 based on conditional generation [29]. The text generation task can be defined as learning a mapping $f: X \longrightarrow Y$ from input X to output Y. Usually, X and Y are sequences of tokens (words), which are denoted by $X = X_1 X_2 \dots X_n$ and $Y = Y_1 Y_2 \dots Y_m$, where $X_i (1 \leq i \leq n)$ and $Y_j (1 \leq j \leq m)$ show the i^{th} and j^{th} token of input and output, respectively. In this kind of problem, the model intends to find Y to maximize the probability (we denote probability of event A by $Pr(A)$ throughout this paper) $Pr_\theta(Y|X)$ based on parameters of the model, θ.

It is possible to insert some additional information in the input of the model. Suppose $P = \{p_1, p_2, p_3, \dots, p_k\}$ is a series of tokens called "prompt tokens" which we prepend to the input X, which gives us the probability $Pr_\theta(Y|[P;X])$. To see the effect of an individual prompt, θ remains fixed. Instead of bounding ourselves to a fixed P, we make P parameterized by θ, and hence it will have its own specific updatable parameters θ_P. This is the basis of the idea of our technique called APC we describe in Section 3.4.

3-3- Multi-Task Leaning (MTL)

As explained in Section 3.1, the expression, agent, and target prediction tasks are related. Previous research [1, 3] stressed the issue of data scarcity and they address it by taking advantage of MTL. We follow them in working with MTL. T5 accepts "prefix" terms, prepended to inputs. Prefixes can be thought as a specific type of prompt (described in Section 3.2). By adding several distinct prompts to the input, we can learn multiple tasks simultaneously, in which we are telling the model what task should be processed, and the model generates output appropriate for that task. When we apply MTL, we are increasing the number of data items (since we can bring in data items for different but related tasks). It can be also considered as a way of data augmentation method. We are comparing this approach to a scenario where a sentence is input into a generative model, and it is expected that the comprehensive output will encompass all tasks.

✉ **Seyed Abolghasem Mirroshandel**
mirroshandel@guilan.ac.ir

3-4- Automatic Prompt Construction (APC)

Inspired by the idea of "prompt tuning" [29], we propose APC approach (as our novel contribution) consisting of two phases:

1) Finding the optimal prompt tokens for a specific task automatically (which is usually called "soft prompt" tuning). We prepend prompt tokens (i.e., tokens of P) to the input tokens, and we try to maximize the likelihood of Y by $Pr_{\theta;\theta_P}(Y|[P;X])$ as the new conditional generation task. By doing backward propagation, gradient updates to the parameter θ_P will take place. After passing input (i.e., X) tokens to the T5 tokenizer, each token is converted to an ID. Then, T5 builds a n by d matrix ($X_e \in \mathbb{R}^{n\times d}$), where n is the length of input tokens and d is the size of embedding vectors contrived for T5 (because T5 comes in different sizes such as small, base, and large). The learnable prompt tokens embedding defined by us are represented as a matrix $P_e \in \mathbb{R}^{k\times d}$. The next thing to do in phase 1 of our method is to append the T5 standard embedding of original input sequence to our updatable prompt embeddings. So, the concatenation of these two forms $[P_e; X_e] \in \mathbb{R}^{(k+n)\times d}$. As a conclusion, in phase 1 only the parameters in P_e are updated.

2) Transferring the optimal prompt tokens learned in phase 1 to be used in the model's fine-tuning. In other words, P_e learned from phase 1 acts as a series of normal tokens, but with the difference that these embeddings representing these tokens might not corresponds to a real word in language. They are new tokens known as "virtual tokens" in the Natural Language Processing (NLP) community.

It should be noted that APC approach is **efficient** regarding the size of trainable parameters. Mathematically, the number of trainable parameters added to the simple fine-tuning is $\mathcal{O}(k \cdot d)$. Even though we consider maximum values, the number of parameters is negligible in comparison to the model parameters when doing fine-tuning.

3-5- MTL + APC

APC can be applied on MTL-based tasks as well. This methodology is our novel contribution. The proposed approach is a combination of fixed prompt (also known as "hard prompt") and soft prompt. More precisely, we extend P a bit more and it is now equal to $P = \{p_1, p_2, p_3, \dots, p_k, p_{k+1}, \dots, p_{k+l}\}$ where the first k tokens are the same trainable tokens as in Section 3.4 which actually is shared among all tasks, and the remaining l tokens are hard prompts that customizes each task.

It is possible to consider a dedicated soft prompt for each task, but our initial experiments indicate no improvement to the results, and furthermore, it is not as efficient as our method in the number of training parameters and runtime. To the best of our knowledge, there are no other similar works for tackling MTL problems in the context of prompt tuning in such a way. In this scenario, the number of tasks does not affect the number of trainable parameters.

As an illustration, Fig. 1 shows the difference between soft prompts and hard prompts. Soft prompts consist of a set of learnable parameters or word embeddings that can be optimized through standard training procedures. In contrast, hard prompts are fixed character strings (i.e., text) that are manually determined and remain constant throughout the process.

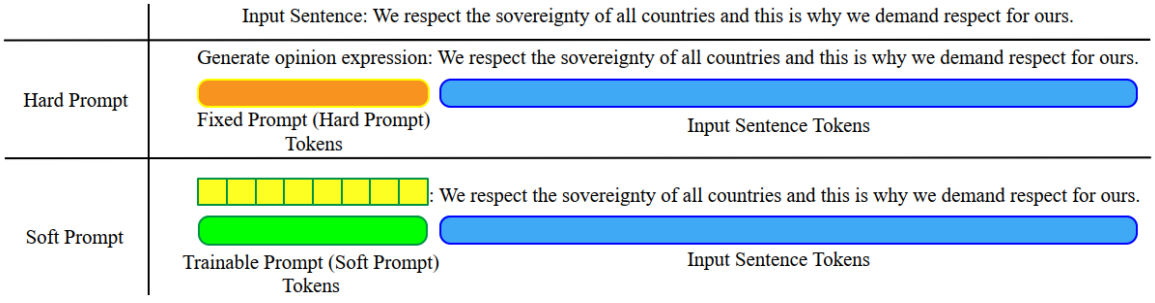


Fig. 1: The comparison between soft and hard prompt.

3-6- Triplet Forming Algorithm

After generating outputs by model, we need to link them in order to find triplets as (expression, role, relation).

3-6-1-End-to-end Setting

In the end-to-end manner, we consider outputs of the expression prediction task as a set of expressions, say $\hat{E}$. Also, the set of predicted agent-expression pairs is designated as $\widehat{AE}$, and set of predicted target-expression pairs as $\widehat{TE}$. We form the set of final predictions as the union of:

$$\{(\xi, \alpha, agent) | \xi \in \hat{E}, (\alpha, \xi) \in \widehat{AE}\} \cup \{(\xi, \tau, target) | \xi \in \hat{E}, (\tau, \xi) \in \widehat{TE}\}$$

which yields us the proper triplets of the task definition presented in Section 3.1. It is notable that when the model predicts an incorrect expression, its agent and target will be ignored in model's evaluation. In other words, correct expression prediction is the precondition for agents and targets evaluation.

3-6-2-Given-Expression Setting

To address the problem in the given-expression setting, we have fed expression with the sentence in the input. Hence, the set of expressions, say E, is revealed and given. With this condition, we only have two outputs: the set of predicted agent items $\hat{A}$, and the set of predicted target items $\hat{T}$. We form the set of final predictions as the union of:

$$\{(\xi, \alpha, agent) | \xi \in E, (\alpha, \xi) \in \widehat{AE}\} \cup \{(\xi, \tau, target) | \xi \in E, (\tau, \xi) \in \widehat{TE}\}$$

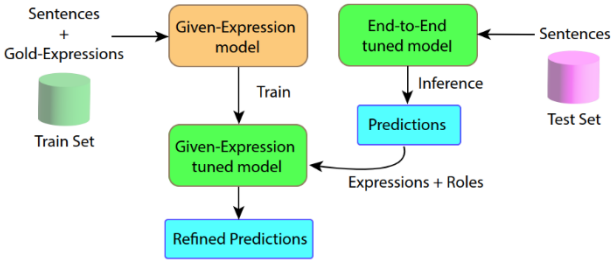


Fig.2: Integrating given-expression model to improve end-to-end predictions by feeding predicted expressions and roles.

3-7- Integrating Given-Expression Model (Int)

As it is shown in Fig. 2, we use predicted outputs of the end-to-end model to be fed into our saved given-expression model in order to see the effect by querying several tasks. It turns out by applying integrating idea, we get a boost in different prediction tasks. In our point of view, based on the error analysis (provided in Section 5.2) and observations of miss-matches, a percentage of false predicted items differs in not important words such as stop-words. Therefore, we believe that the fine-tuned end-to-end model outputs are of sufficiently high quality to accurately identify expression spans, even though some words at the beginning or end may occasionally be omitted. Performance of our system in the given-expression setting demonstrates its excellence as well. By supplying these expressions to the given-expression model, we can identify those that closely resemble gold standard expressions and determine the corresponding roles for each one. Then, by comparing the new predictions with the old ones, we can revise the predictions. This revision process mainly relies on the correlation rate between the two sets of predictions and is based on the improvements observed in the development set performance. We suggest this application of models to be considered as a novel idea of Transfer Learning in NLP.

In this part of our research, we explain the dataset we exploited, the evaluation metrics we report, the setup of our experiments and other details involving training procedure.

3-8- Dataset and Settings

As mentioned earlier, we employed the most frequently used dataset, MPQA 2.0, in order to carry out our experiments. We mimic the data split of previous work [9, 3, 8, 2] and conduct 5-fold cross-validation run. We set the random seed to a constant number to make the results reproducible. It's worth mentioning that, in line with prior research as well as considering the intricate complexity and granularity of the MPQA, our exclusive focus has been on this dataset.

Our models were developed using the PyTorch [1] deep learning framework and we performed the models on a single NVIDIA A100-SXM4-40GB GPU. We also utilized packages such as spaCy[2] and NLTK[3], along with the scikit-learn library [4], NumPy [5], and Matplotlib [6]. The T5-base model and its tokenizer, which were obtained from the

[1] https://pytorch.org/
[2] https://spacy.io/
[3] https://www.nltk.org/
[4] https://scikit-learn.org/stable/
[5] https://numpy.org/
[6] https://matplotlib.org/

✉ **Seyed Abolghasem Mirroshandel**
mirroshandel@guilan.ac.ir

Hugging Face Transformers library[1], were also employed in our implementation.

3-9- Details of Input/Output Design

Since we are using T5 to solve this OM problem in the generative way, the design of input and output structure is essential. Hence, we will go into detail by examples in this section. Please note that samples of input and output are presented here are real ones used in implementations. To develop the input, we use prompts to make tasks distinguishable and more learnable by T5. In the end-to-end approach, we use one prompt set, but it also possible to have more. For the given-expression setting, we give the sentence and the expression using two different prompt sets. Upper parts of Fig. 3, 4, and 5 indicate input structure used in our system. At the output, in the end-to-end setting we use "=" (equal sign) to show allocation of an opinion role (agent/target) to an expression, i.e. "agent1 = expression1". If there are more than one item, we split them by "|" (pipe) symbol. It operates precisely in accordance with the triplet forming algorithm described in the end-to-end setup (Section 3.6.1). Finally, for the given expression manner, we only divide opinion role spans by "|" sign. As depicted in the lower part of Fig. 3, outputs for opinion roles are forming pairs of (role, expression), which are grouped with the "=" character. It functions accurately in alignment with the triplet forming algorithm outlined in the given-expression setup (Section 3.6.2). Despite this configuration and design of this type of output reflecting the concept pretty well, it also results the best among other choices we examined in our initial experiments.

Nevertheless, we do not require the expression prediction sub-task to produce its outputs in this way. The reason we are doing this is to make a harmony between all of tasks' outputs. It seems if input and output of several tasks at hand executing by T5, be quite identical in format, the model performs better. For illustration, see Fig. 3, 4, and 5. Prefixes are highlighted in red. Sentences are highlighted in aqua. Opinion roles and expressions are highlighted in yellow and green respectively. Prefix (prompt) phrases are depicted in all pictures are examples and they could get changed and replace by the APC mechanism. In our assertion that the fixed set of prompts could be substituted by the APC mechanism, we are referring to a system that automatically adds a collection of learnable vectors to the prompts throughout the training process. These vectors are dynamically updated, thereby improving the model's performance across various tasks. It is essential to highlight that these vectors may not directly represent actual words (unlike our standard prompt words); rather, they exist exclusively within the embedding space and are inserted at appropriate positions in the input sequence when converting words into their embedding vectors.

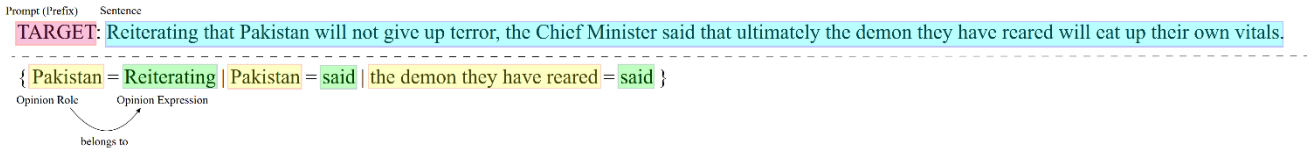


Fig. 3: An example of input (up) and output (down) with multiple opinion role-expression pairs used in the experiments in the end-to-end setting.

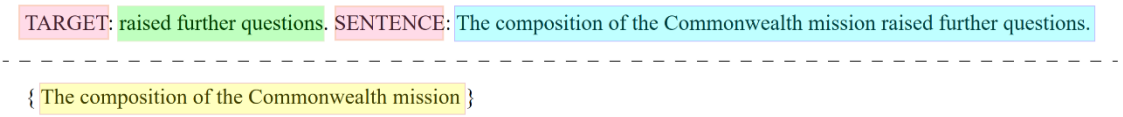


Fig. 4: An example of input (up) and output (down) with one opinion role used in the experiments in the given-expression setting when querying its targets

[1] https://github.com/huggingface/transformers

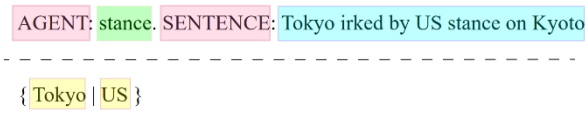


Fig. 5: An example of input (up) and output (down) with two opinion roles used in the experiments in the given-expression setting when querying its agents.

3-10- Hyper-parameters and Training Details

The number of prompt tokens is an important hyper-parameter in our experiments. We tried different number of tokens in our experiments (i.e., 20, 50, 100, and 150 tokens). In the end-to-end setting, we get the best results with 100 tokens. On the other hand, in the given-expression setting, the results are reported using 20 tokens. Dropout rate of T5 transformer equals to its default value. The batch size is 16 and we use the Adam optimizer. The learning rate (LR) and number of epochs (Epochs) for each model are depicted in Table 2. The loss function considered for training is the default one for training T5 models. We select the model (or those weights we require) that performs best on the development set data.

By following previous research on the issue of prompt tokens initialization [30, 29], we categorize all methods in three groups: 1) Uniformly sample from the range $[-0.5, 0.5]$. 2) Select from vocabulary (or a specific subset of the whole vocabulary). 3) Select from class labels. As we do not encounter a classification problem, we only tested methods 1 and 2. In the experiments, we did not observe a notable variation in the results. Therefore, due to the quicker convergence of method 2, we chose to sample random tokens from the vocabulary.

Table 2: Learning rate and epoch number count of different models.

Model Type	LR	Epochs
End-to-end fine-tuning	1e-4	70
Given-expression fine-tuning	1e-4	100
Prompt tokens learning	0.3	300

3-11- Evaluation Metrics

To keep up with previous works (e.g., Xia et al. [3]) and make our results comparable, we employ Precision, Recall, and F1 score (in some cases, we only show F1) to evaluate our experimental results using the Exact match setting (i.e., *Exact P, R, and F1*), in which we have a true positive (TP) for calculating recall and precision if and only if the entire sequence of tokens is predicted exactly. Additionally, we utilize two auxiliary metrics known as Binary (i.e., *Binary F1*) and Proportional match (i.e., *Proportional F1*). The proportional metric measures the maximum portion that a predicted item matches its gold-standard item, and counts this fraction as a TP in calculating recall and precision. The binary metric yields a TP if a predicted sequence overlaps with its gold-standard sequence in at least one token. We present the formulas for Precision, Recall and F1 score as follows.

$$Precision = \frac{TP}{TP + FP} \quad (1)$$

$$Recall = \frac{TP}{TP + FN} \quad (2)$$

$$F1 = 2 * \frac{Precision * Recall}{Precision + Recall} \quad (3)$$

4- Results Analysis and Discussion

In this section, the experimental results in both end-to-end and given-expression settings are presented. Furthermore, we compared our method with other established successful methods. In the proceeding tables, “GenOM” shows our proposed method and “Standalone” shows that the model solely predicts expressions. “MTL”, “Prompt”, and “Int” show our multi-task learning, automatic prompt construction, and integration ideas, respectively. “+” sign indicates the combination of certain methods within our approach. In the end-to-end setting, we compare our results to: BiLSTM-CRF1 [23], Trans [25], SpanOM [3], PtrTrans [9], and BiLSTM-CRF2 [24] methods.

In the given-expression setting (i.e., ORL problem), we also compare our results to: EnhanceORL [8], SynAwareORL [2], and ORL [1] methods. “BERT” means integrating BERT representations into the model. Also, some methods utilized external knowledge as: i) “SynCons” means syntactic constituent features. ii) “Syn” means syntax-enhanced version. iii) “SynDep” means dependency syntax knowledge. iv) “SRL” means Semantic Role Labeling that involves semantic knowledge.

The best results are in bold. The best results <u>without involving any external knowledge</u> are underlined.

✉ **Seyed Abolghasem Mirroshandel**
mirroshandel@guilan.ac.ir

4-1- Results in the end-to-end Setting

The results from Table 3 show a substantial improvement when we apply MTL on the expression prediction task. To follow, F1 score of "Standalone" from 61.4% boosts up to 62.8% when we use MTL method. Also, we observe a 3.6% increase when we adopt APC and MTL jointly. Furthermore, leveraging integration method improves the result by 0.5 percent and set the new SOTA for expression prediction task. The APC method also demonstrates a notable improvement itself. This is evident when comparing the F1 scores of the "Standalone + Prompt" to the "Standalone", which shows a notable increase of 2.8%. This observation emphasizes the effectiveness of our proposed APC method.

Another point of achievement in our methods, is the convergence of Precision and Recall. These two measures are both going up and shows a successful balance between them, which helps to gain the SOTA performance on F1 score. Although the highest Precision was achieved by "SpanOM + Prompt" model, but the low value of Recall lowers their F1 score.

Table 3: Results and comparison of the expression prediction on the exact match metric in the end-to-end setting. "-" means results are not reported in their paper.

Models	Exact Match		
	P	R	F1
Trans	60.2	48.5	53.0
SpanOM	64.9	52.6	58.1
SpanOM + BERT	**67.2**	60.6	63.7
PtrTrans	-	-	58.1
PtrTrans + Syn	-	-	59.9
PtrTrans + BERT	-	-	63.9
PtrTrans + BERT + Syn	-	-	65.3
GenOM			
Standalone	62.0	61.0	61.4
Standalone + Prompt	64.6	63.9	64.2
MTL	63.2	62.5	62.8
Prompt + MTL	64.5	65.5	65.0
Prompt + MTL + Int	65.1	**65.9**	**65.5**

On the other hand, in opinion roles prediction (Table 4), in overall value of all metrics (i.e., exact and auxiliary), we outperform other systems and set a new SOTA performance. In all auxiliary metrics (i.e. proportional and binary) our results are superior compare to other related research. In Exact matching, agent performance is remarkably better than the history of results, however we could achieve second best and best without using external knowledge for target role.

Generally, we observe a considerable improvement in all conditions when we adopt each of our novel ideas. This magnifies our enunciation about using raw text-to-text transformer in the correct way.

Table 4: Experimental results of our GenOM system and comparison with previous research works on the MPQA 2.0 benchmark dataset in the end-to-end setting. "-" means results are not available and/or not presented in their paper.

Model	Exact F1			Binary F1			Proportional F1		
	Overall	Agent	Target	Overall	Agent	Target	Overall	Agent	Target
BiLSTM-CRF1	-	-	-	-	58.2	55.0	-	-	-
Trans	-	47.0	31.5	-	60.9	56.4	-	-	-
SpanOM	43.1	52.9	32.4	51.0	56.5	45.1	48.9	55.6	41.7
PtrTrans	43.7	53.2	33.2	-	57.9	47.0	-	56.9	42.8
PtrTrans + Syn	44.4	54.7	35.0	-	58.3	47.7	-	57.1	43.6
BiLSTM-CRF2 + BERT	-	-	-	-	55.5	50.4	-	46.6	34.3
SpanOM + BERT	49.9	58.2	41.1	57.8	62.0	53.3	55.7	61.2	49.9
SpanOM + BERT + SynCons	50.5	58.5	41.8	-	-	-	-	-	-
PtrTrans + BERT	50.1	58.3	42.0	-	62.3	53.7	-	61.7	50.4
PtrTrans + BERT + Syn	51.6	59.5	44.0	-	63.2	55.2	-	62.3	52.0
GenOM									
MTL	46.4	56.2	36.8	56.6	60.4	52.8	53.4	59.5	47.4
Prompt + MTL	48.9	58.3	39.8	60.0	63.1	57.0	56.8	61.8	51.9
Prompt + MTL + Int	51.8	61.1	42.6	62.5	65.3	59.7	59.4	64.3	54.6

4-2- Results in the given-expression setting

As shown in Table 5, our system achieves SOTA results for all opinion roles (overall, agent and target) using all metrics. By adopting MTL, we obtain new SOTA results for agent and overall using the exact match metric, but we are not better in target. After applying APC, we observe a substantial boost in F1 score, so that on exact match, we establish a new SOTA for overall, agent and target.

4-3- Discussion and Error Analysis

By running an error analysis on the predicted items in development set, which is depicted in Table 6, we understand that a considerable portion of wrong matches are due to the mismatch of opinion expressions. Hence, we aim to focus more deeply on expression prediction task in future. Although Unmatch (means no overlap) items seems to be legitimate errors, but we observe some samples which the system prediction and gold-standard are actually pointing to one specific entity. As an illustration, consider the sentence No.1 from Table 7. Our system predicts "he" as an agent for expression "said", but the gold-standard agent for this expression is "Syed Hamid". Note that in this sample, system successfully determined the gold-expression. Obviously, "he" corresponds to "Syed Hamid" and they are actually one unique entity. Therefore, it seems leveraging "Anaphora resolution" techniques could be helpful and correct some miss-matches. As it is reported in Table 5, partial matches are also considerable. Our analyses indicate a variety of conflicts between the predicted and gold-standard occurs at the boundaries but the interesting point is that most of these discrepancies are about stop-words. We did an automatic analysis by using *Levenshtein distance algorithm* in order to align predicted and gold-standard spans and find disparate segments between them. The most frequent words causing discrepancies in target are *to, the, a, and, of, in, on, is, be*, and in agent are *the, of, and, an, at, a*. In the expression prediction task, the rate of partial errors is higher, and the discrepancies are also the same. The most common words that cause conflict in expression prediction task are *to, of, the, is, are, by, a, in*.

Table 5: Experimental results of our GenOM system and comparison with previous research works on the MPQA2.0 benchmark dataset in the given-expression setting. "-" means results are not available and/or not presented in their paper

Model	Exact F1			Binary F1			Proportional F1		
	Overall	Agent	Target	Overall	Agent	Target	Overall	Agent	Target
EnhanceORL	58.3	73.1	42.7	75.2	81.6	68.3	70.6	79.4	61.2
SynAwareORL	58.8	73.1	44.2	75.4	81.2	69.5	71.0	79.3	62.5
SpanOM	59.6	72.4	45.8	71.6	78.1	64.5	68.1	76.7	58.7
ORL + SRL	61.5	75.6	46.4	-	-	-	-	-	-
EnhanceORL + SRL	63.7	77.0	51.0	-	-	-	-	-	-
SynAwareORL + BERT	64.7	76.7	52.6	80.6	85.5	75.7	76.5	83.6	69.3
SynAwareORL + BERT + SynDep	68.1	79.5	56.6	-	-	-	-	-	-
SpanOM + BERT	66.0	76.5	55.0	77.9	82.7	72.9	74.6	81.5	67.4
SpanOM + BERT + SynCons	68.0	78.3	57.0	-	-	-	-	-	-
GenOM									
MTL	68.2	79.3	56.7	84.1	87.5	80.6	79.4	85.5	73.0
Prompt + MTL	68.7	79.9	57.1	84.3	87.8	80.7	79.5	85.7	73.2

Table 6: Percentage of different types of errors among all predicted items of development set in each task. EM stands for Expression Miss-match, PM stands for Partial Match and U means Unmatch or legitimate errors

Task	EM	PM	U
Agent	55.7	15.5	28.8
Target	39.3	30.4	30.3
Expression	-	57.7	42.3

As reported in other studies like Xia et al. [3], we also observed some peculiarities and errors in annotations of MPQA, which might provide false information to our system. For instance, sentence No.2 from Table 7, there is an expression marked in corpus as "The", but we think "The" is not a reasonable expression. On the other hand, in some sentences, there are predictions by our system which seems to be correct but they are absent in annotated data. For instance, consider sentence No.3 from Table 7. The system predicted the agent of "oppose" expression as "many poor" which is correct. But there is not any agent marked for this expression in the corpus. To mitigate these **gold errors** in the future, it is crucial to enhance the quality

✉ **Seyed Abolghasem Mirroshandel**
mirroshandel@guilan.ac.ir

of MPQA annotation. This improvement will pave the way for more accurate and reliable results.

We also did some preliminary experiments with a variant of T5, called FLAN-T5 [19], but the results did not indicate superiority.

Our proposed generative approach utilizing the T5 transformer in conjunction with MTL and APC shows notable performance enhancements on the MPQA 2.0 dataset. However, several limitations must be addressed for application in real-world scenarios. First, the model's dependence on specific characteristics of the dataset may restrict its adaptability to other domains where opinion structures vary significantly or where annotated data is limited. Additionally, the complexity and computational requirements of the generative model could present challenges for deployment in resource-limited environments or in applications that necessitate real-time processing. Moreover, while APC effectively optimizes prompts for this dataset, its performance in entirely different contexts or languages may differ, requiring further tuning or adaptation.

Table 7: Some sentences of MPQA 2.0 corpus.

No.	Sentence
1	Syed Hamid said the international community must deal with terrorism rationally and form a new "security architecture" to combat what he described as a "new dimension of crime against humanity" in the long term.
2	The CIA was given the task to topple governments and install rulers of its own choice.
3	However, 78 percent of those polled believe there are many poor who oppose him.

5- Conclusion and Future Work

This research introduces a novel generative framework for opinion mining, leveraging the T5 transformer model through Multi-Task Learning (MTL) and Automatic Prompt Construction (APC). Our approach achieves remarkable performance improvements on the MPQA 2.0 dataset, setting new state-of-the-art records without relying on external knowledge. The MTL strategy enables the model to learn interconnected sub-tasks concurrently, enhancing the detection of opinion expressions and their associated roles. Meanwhile, APC facilitates the automatic optimization of prompts, effectively addressing the challenges posed by manual prompt engineering and ensuring more efficient task customization. The results indicate that the synergy between MTL and APC significantly elevates precision, recall, and F1 scores across various evaluation metrics. By integrating predictions from both the end-to-end and given-expression settings, our method achieves a more accurate recognition of opinion structures. These findings highlight the effectiveness of generative models in capturing complex opinion relationships within text.

Looking ahead, future research can build on these findings by integrating additional syntactic and semantic knowledge into generative models and further refining the APC technique. Extending the application of our methods to other datasets and domains is also critical. Investigating the use of more advanced generative transformers or combining our approach with alternative machine learning strategies could yield additional improvements. Furthermore, enhancing the quality of existing datasets and developing new benchmarks will be essential for validating the generalizability and effectiveness of these methods across a broader range of contexts.

Reference

[1] A. Frank and A. Marasović, "SRL4ORL: Improving Opinion Role Labeling Using Multi-Task Learning with Semantic Role Labeling," in Proceedings of the 2018 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, New Orleans, Louisiana, 2018.

[2] B. Zhang, Y. Zhang, R. Wang, Z. Li and M. Zhang, "Syntax-Aware Opinion Role Labeling with Dependency Graph Convolutional Networks," in Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics, Online, 2020.

[3] Q. Xia, B. Zhang, R. Wang, Z. Li, Y. Zhang, F. Huang, L. Si and M. Zhang, "A Unified Span-Based Approach for Opinion Mining with Syntactic Constituents," in Proceedings of the 2021 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Online, 2021.

[4] S. Ahmadnia, A. Yousefi Jordehi, M. Hosseini Khasheh Heyran, S. Mirroshandel and O. Rambow, "Opinion Mining Using Pre-Trained Large Language Models: Identifying the Type, Polarity, Intensity, Expression, and Source of Private States," in Proceedings of the 2024 Joint International Conference on Computational Linguistics, Language Resources and Evaluation (LREC-COLING 2024), Torino, Italia, 2024.

[5] J. Wiebe, "Identifying subjective characters in narrative," in COLING 1990 Volume 2: Papers presented to the 13th International Conference on Computational Linguistics, 1990.

[6] J. Wiebe, T. Wilson and M. Bell, "Identifying collocations for recognizing opinions," in Proceedings of the ACL-01 Workshop on Collocation: Computational Extraction, Analysis, and Exploitation, 2001.

[7] T. A. Wilson, Fine-grained subjectivity and sentiment analysis: recognizing the intensity, polarity, and attitudes of private states, University of Pittsburgh, 2008.

[8] M. Zhang, P. Liang and G. Fu, "Enhancing Opinion Role Labeling with Semantic-Aware Word Representations from Semantic Role Labeling," in Proceedings of the 2019

Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies,, Minneapolis, Minnesota, 2019.

[9] S. Wu, H. Fei, F. Li, D. Ji, M. Zhang, Y. Liu and C. Teng, "Mastering the explicit opinion-role interaction: Syntax-aided neural transition system for unified opinion role labeling," in Proceedings of the AAAI conference on artificial intelligence, Online, 2022.

[10] Z. Gao, A. Feng, X. Song and X. Wu, "Target-Dependent Sentiment Classification With BERT," IEEE Access, vol. 7, pp. 154290-154299, 2019.

[11] Y. Z. R. W. Z. L. M. Z. Bo Zhang, "Syntax-Aware Opinion Role Labeling with Dependency Graph Convolutional Networks," in Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics, Online, 2020.

[12] W. Zhang, X. Li, Y. Deng, L. Bing and W. Lam, "Towards Generative Aspect-Based Sentiment Analysis," in Proceedings of the 59th Annual Meeting of the Association for Computational Linguistics and the 11th International Joint Conference on Natural Language Processing, Online, 2021.

[13] X. Bao, W. Zhongqing, X. Jiang, R. Xiao and S. Li, "Aspect-based Sentiment Analysis with Opinion Tree Generation," in Proceedings of the Thirty-First International Joint Conference on Artificial Intelligence, Vienna, 2022.

[14] P. Kavehzadeh, M. M. Abdollah Pour and S. Momtazi, "Deep Transformer-based Representation for Text Chunking," Journal of Information Systems and Telecommunication (JIST), vol. 3, pp. 176-184, 2023.

[15] S. Chakraborty, M. Borhan Uddin Talukdar, P. Sikdar and J. Uddin, "An Efficient Sentiment Analysis Model for Crime Articles' Comments using a Fine-tuned BERT Deep Architecture and Pre-Processing Techniques," Journal of Information Systems and Telecommunication (JIST), vol. 12, pp. 1-11, 2024.

[16] N. Jadhav, "Hierarchical Weighted Framework for Emotional Distress Detection using Personalized Affective Cues," Journal of Information Systems and Telecommunication (JIST), vol. 10, pp. 89-101, 2022.

[17] Liu, C. Raffel, N. Shazeer, A. Roberts, K. Lee, S. Narang, M. Matena, Y. Zhou, W. Li and P. J., "Exploring the Limits of Transfer Learning with a Unified Text-to-Text Transformer," Journal of Machine Learning Research (JMLR), vol. 21, no. 140, pp. 1-67, 2020.

[18] M. Lewis, Y. Liu, N. Goyal, M. Ghazvininejad, A. Mohamed, O. Levy, V. Stoyanov and L. Zettlemoyer, "BART: Denoising Sequence-to-Sequence Pre-training for Natural Language Generation, Translation, and Comprehension," in Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics, Online, 2020.

[19] H. W. Chung, L. Hou, S. Longpre, B. Zoph, Y. Tay, W. Fedus, Y. Li, X. Wang, M. Dehghani, S. Brahma, A. Webson, S. S. Gu, Z. Dai, M. Suzgun, X. Chen, A. Chowdhery, A. Castro-Ros and Marie, "Scaling instruction-finetuned language models," arXiv preprint arXiv:2210.11416, 2022.

[20] E. Breck, Y. Choi and C. Cardie, "Identifying expressions of opinion in context.," in International Joint Conference on Artificial Intelligence, Hyderabad India, 2007.

[21] B. Yang and C. Cardie, "Joint Inference for Fine-grained Opinion Extraction," in Proceedings of the 51st Annual Meeting of the Association for Computational Linguistics, Sofia, Bulgaria, 2013.

[22]B. Yang and C. Cardie, "Joint Modeling of Opinion Expression Extraction and Attribute Classification," Transactions of the Association for Computational Linguistics, p. 505–516, 2014.

[23] A. Katiyar and C. Cardie, "Investigating LSTMs for Joint Extraction of Opinion Entities and Relations," in Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics, Berlin, Germany, 2016.

[24] W. Quan, J. Zhang and X. T. Hu, "End-to-end joint opinion role labeling with bert," in IEEE International Conference on Big Data (Big Data), 2019.

[25] M. Zhang, Q. Wang and G. Fu, "End-to-end neural opinion extraction with a transition-based model," Information Systems, vol. 80, pp. 56-63, 2019.

[26] J. Devlin, M.-W. Chang, K. Lee and K. Toutanova, "Bert: Pre-training of deep bidirectional transformers for language understanding," in Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Minneapolis, Minnesota, 2019.

[27]O. Vinyals, M. Fortunato and N. Jaitly, "Pointer networks," Advances in neural information processing systems, vol. 28, 2015.

[28] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, {. Kaiser and I. Polosukhin, "Attention is all you need," Advances in neural information processing systems}, vol. 30, 2017.

[29] B. Lester, R. Al-Rfou and N. Constant, "The Power of Scale for Parameter-Efficient Prompt Tuning," in Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing, Online and Punta Cana, Dominican Republic, 2021.

[30] D. C. Senadeera and J. Ive, "Controlled text generation using T5 based encoder-decoder soft prompt tuning and analysis of the utility of generated text in AI," in arXiv preprint arXiv:2212.02924, 2022.

Journal of Information Systems and Telecommunication
Vol.12, No.3, July-September 2024, 197-207
http://jist.acecr.org
ISSN 2322-1437 / EISSN:2345-2773

A Survey of Intrusion Detection Systems Based On Deep Learning for IoT Data

Mehrnaz Moudi[1,*], Arefeh Soleimani[1], Amir Hossein Hojjatinia[1]

[1]. Department of Computer Engineering, University of Torbat Heydarieh

Received: 25 Oct 2023/ Revised: 04 Jul 2024/ Accepted: 11 Aug 2022

Abstract

Today, the scope of using the Internet of Things is growing by taking science and technology as the first place in human life, and as these networks get bigger, more data are exchanged. It performs high-speed data exchanges on the Internet and in a pre-defined network. The more the Internet of Things penetrates into people's lives, the more important data it transmits. This causes attackers to draw attention to these data, and Internet of Things network devices that have limited resources are exposed to attacks. With the complexity of hardware and software for the ease of human's use, naturally more intelligent attacks will happen, which is the reason of presenting many methods in this field. For this reason, in this article, we are going to discuss the most important methods used in intrusion detection systems based on deep learning and machine that can identify these interruptions. In this article, we have compared 46 articles from 2020 to 2024 based on the type of dataset used, the type of classification (binary or multi-class) and the accuracy rates obtained from each method, and we have been able to see a comprehensive overview for researchers who intend to work in IoT data security. According to the obtained results, if the proposed method is implemented in binary form, it can achieve better accuracy than multi-class.

Keywords: Internet of Things; Artificial Intelligence; Machine learning; Deep learning; Intrusion Detection Systems.

1-Introduction

We are in the 21st century, where science and technology take the first place in human life. From the past to today, science has made significant progress in various fields in order to improve human comfort. The Internet of Things (IoT) technology is one such advancement in science. Where humans no longer have control over objects and we have a relationship between objects, and the relationship between humans and objects has no meaning. This is one of the signs of increasing the use of artificial intelligence in our earthly world. Today, artificial intelligence and machine learning have penetrated human life so much that the theory can be put forward that increasing the power of artificial intelligence can in some way bring about the well-being of humans and bring about the day when this same artificial intelligence against humans. IoT is not an exception to this rule and has been able to use deep learning algorithms and create a series of artificial neural networks such as CNN[1], RNN, NN[2], LSTM[3], MLP, which are similar to human brain nerves and have a series of weights.

IoT performs high-speed and real-time data exchanges on the Internet and in a pre-defined network [1]. In this network, a set of smart devices that are not limited to a geographical area are exchanging information [2]. Due to the many advantages of IoT, it is used in various government organizations, people's personal lives, health and treatment, industry and military organizations, and transportation and airways and seaways, and depending on the type of data exchanged and their importance as well as to maintain their security, various security protocols are expected for this type of networks [3, 4]. Due to the volume of important generated data that is exchanged based on IoT technology [5], the field of attack and information theft is also provided for hackers and makes the network vulnerable to electronic attacks and security challenges [3]. In the past, traditional methods such as the use of antiviruses and firewalls were used to deal with the security of network objects. However, for example, a smart watch that is connected to the Internet and connected with other devices does not have such a suitable and powerful hardware and processor that can install heavy security programs on it. Due to the hardware and processor limitations of this category of devices, as well as the ability

[1] Convolutional neural networks
[2] Neural Network
[3] Long short-term memory

✉ **Mehrnaz Moudi**
mehrnazmoudi@gmail.com/mmoudi@torbath.ac.ir

to respond quickly, which is one of the most important features of IoT [1], IDS[4] has been provided to monitor the network, the incoming and outgoing traffic from the network. In addition, if abnormal behaviors and anomalies are detected, quickly identify them and find a solution for intrusions. Usually, a group of security experts controls the network of IDS, and the detected flows are reported to the security expert that he provides a series of suggestions to deal with the detected intrusion based on decision-making systems.

Consequently, in order to design practical IDS, we need to know artificial networks based on deep learning so that we can use data mining to obtain the order governing reliable datasets that contain normal conditions and under attack, and the patterns. These datasets are embedded in the data mining science and entered into the desired neural network so that we can identify malicious or normal traffic and make the system resistant to future intrusions. In addition, sometimes the detection of these intrusions and countermeasures require quick action, for example, fire alarm systems, which are extremely important, need to be equipped with more advanced IDS [6]. Generally, when a new method is invented or optimized in this field, they are tested with previously created datasets such as N-BaIoT, IoTID20, NSL-KDD, UNSW-NB15, CICIDS2018 [7-9] and based on a series of parameters such as Accuracy, F-score, Recall, they evaluate the proposed method and compare the results obtained with previous methods.

The reason that many methods have been presented in this field is that with the passage of time and the complexity of hardware and software for the ease of use for humans, naturally more intelligent attacks will happen to these devices. Fundamentally, the ease of using the tool follows complex activities in the background and provides more scope for penetration. One of the best methods that is derived from mathematical calculation principles and has moved towards becoming intelligent is the methods that are based on deep learning [5]. Because in this method, by using multiple hidden layers, we can obtain useful features of network traffic and better detect intrusions. However, due to the amount of unstructured data produced by IoT devices [5], many researches have been conducted to extract the important and key features of the data with the help of deep learning techniques. IDS are used when network intrusion has occurred and we intend to find them, but security protocols such as firewalls and antiviruses prevent malware from entering the network. As a result, the common solutions based on deep learning are still facing many challenges and each of them has a series of disadvantages and limitations and for this reason, new and more optimal methods in this field based on learning are being developed day by day. Deep learning is more reliable than other methods because it can easily extract the important information of the dataset and hence provides better accuracy.

In this article, we have reviewed 46 articles from reputable journals that have presented between 2020 and 2024 in the field of IDS based on deep learning algorithms in IoT and categorized them based on various parameters. For the convenience of researchers, in this article, we examine the different dimensions of IDS and examine the new algorithms that have been presented and compare them. Investigations of ours provide deep learning-based intrusion detection in IoT. To the best of our knowledge, this is the only survey paper that has so far conducted a comprehensive study on deep learning-based security solutions with analytics. As well as this article gives researchers a very important and unique overview compared to other previous reviews. Considering that the methods presented in this field are implemented both in binary and multi-class form, it was necessary for us to let compare the articles in the last 4 years that have studied in the field of intrusion detection from the point of view of being binary and multi-class and see which of these two methods can provide higher accuracy.

In the continuation of the introduction section, we will organize the sections of the article. In section 2, we present a hierarchical view of the subject, in which we have sub-sections that fully explain each area. In section 3, we have examined the solutions and challenges of deep learning and presented a comprehensive table that includes the comparison of methods. Section 4 is our discussion in which we discussed the evaluation parameters of the methods. In conclusion, Section 5, which is the last section, is our conclusion based on the evaluations.

2-Hierarchical View of Intrusion Detection Systems

In this section, we intend to take a hierarchical view of IDS and explain in detail all the components that play a role in creating IDS. For this purpose, first in section A, we have presented the importance of learning data mining science and in section B; we have discussed the applications of artificial intelligence. Then, in section C, it is time to examine machine learning, which we have described its various uses and categories, and next in section D, it is time to get to the core of our article, which is deep learning. Finally, in section E,

[4] Intrusion Detection System

we have discussed the importance of using IDS using deep learning algorithms.

2-1- Details of Data Mining and its salient features

In the past, the use of electronic and digital tools was not as widespread as it is today. Thus, research on the data generated by this tool was not much discussed. The digital age can be called the 1990s, where digital devices produced a huge amount of data [10]. However, today, we see traces of digital in every environment and place we look. Naturally, this widespread use of these devices leads to the production of a series of data in massive volumes. The mass data that is output from these devices contains useful information about the system. This obtained information is often not understandable for humans. In the past, due to the minimal use of digital tools, the output data was also small, and humans used to analyze the data with a superficial look and manual separation. Gradually, with the significant increase in the use of digital tools, data was produced in huge volumes. Therefore, when the time came for these data to be analyzed by humans for better performance, he would get confused and unable to calculate. For this reason, the science of data mining was proposed. Data mining is a process to find anomalies, associations, patterns, changes, structures, correlations and non-correlations in datasets with massive data [10]. Among the most important datasets with large data are N-BaIoT, IoTID20, NSL-KDD, UNSW-NB15, CICIDS2017, CICIDS2018, KDDCup99, MQTT IOT IDS2020, KDD, Bot-IOT, KDD99, MQTT.

Data mining was able to provide a series of methods and methods to human, enabling him to find the law and order governing the data, and this human being analyzed these data through a series of evaluations in order to be able to find the pattern governing these data and classify them [10, 11]. If we can analyze these data generated from digital devices well and find the rules on them, we can optimize the system for the next time in order to reach the goals with more optimal power. The science of data mining was also created in order to be able to extract these ruling patterns from the data by providing a series of methods and methods such as artificial intelligence, deep learning, and so on. For example, a company that operates in the field of investment can perform a series of analyzes to predict the price trend of a stock by analyzing the data obtained from the chart of each stock [10]. On the other hand, in another example, we can refer to the data generated by the IoT. IoT devices produce massive amounts of data in the form of datasets, and it is quite difficult to check each one of them by humans. With the data mining of these datasets, it is possible to find the order governing them and inform IDS. The main data mining techniques include the following:

1. Data cleaning
2. Classification
3. Clustering
4. Regression
5. Prediction
6. Decision trees
7. Neural networks
8. Long-term memory processing

2-2- Details of Artificial Intelligence and its salient features

Artificial intelligence is one of the most interesting research fields in computer science and many researchers have done many activities in this field. It is enough to prove the exactingness of the research field of artificial intelligence that according to the report of the online portal, the statistics of the global market of artificial intelligence software will increase from 9.51 billion dollars in 2018 to 118.6 billion dollars by 2025 [12]. If we want to apply this concept of artificial intelligence, it is better to first separate this word into artificial and intelligence. Intelligence includes the ability to think and learn based on experience, and everything that is made by human thought and intelligence is called artificial [16]. Now, the combination of these two words helps us to understand the main concept of artificial intelligence more clearly. Artificial intelligence is a set of algorithms that are given by humans to a series of robots or programs so that they can learn with the help of these primary algorithms by means of pre-produced data sets and understand the pattern governing the data by repeating and reviewing these algorithms. Eventually they will be able to optimize their performance and make decisions without human intervention according to the educational experience that they have gained in the previous stage and it is no longer necessary for humans to dictate commands to the program or robot one by one.

The techniques used in artificial intelligence are [13]:

- machine learning
- Deep learning
- Decision tree techniques
- Support Vector Machine (SVM)
- Fuzzy Logic
- Genetic algorithm
- Bayesian network
- Clustering techniques

Therefore, in the discussion of identifying intrusions, we can use the techniques used in artificial intelligence, such as machine learning, which means the ability to teach a machine by learning algorithms, and deep learning, which means simulating the neural networks of the human brain, and has many advantages over other techniques are being used for IoT data.

2-3- Details of Machine Learning and its Salient Features

In fact, machine learning is a subset of artificial intelligence. Since it was said in the previous sections, with the help of machine learning algorithms, the system can be enabled to receive and read the data by itself without direct programming, and at the end, the output along with a series of suggestions for better decision-making offer to the user. In general, the basis of machine learning techniques is that they intend to improve performance over time based on previous results [13] and automate processes [14]. Recently, machine learning, like artificial intelligence, has been interested in university research and has been able to solve problems in real-world businesses largely [15]. The main machine learning techniques include the following [13]:

- Neural Network (NN)
- Bayesian network
- Markov model
- Vector machine support

In addition, various types of machine learning [14]:
- Supervised learning
- Unsupervised learning
- Reinforcement learning

2-4- Details Deep Learning and its Salient Features

Deep learning is a more complex part of machine learning. In most definitions, these two concepts are considered the same, but in reality, they are not, and each of them has a series of unique characteristics. As mentioned, deep learning is a set of neural nodes, each of which can be a type of input to a neural network. Generally, deep learning consists of neural networks that have three layers. The first layer is the neural nodes or our inputs to the network and after that, we have hidden layers and finally the output layer, which are considered as inputs for the next layers. The hidden layers extract features of nodes in different ways. In other words, the central core of neural networks are the hidden layers that are placed between the input and output layers and have activation functions. Because in this layer we can extract the features from the inputs in different ways. For example, the hidden layer in convolutional neural networks has a series of multi-dimensional inputs that we can obtain in the hidden layer with the help of a large number of filters important features of the input data. In the traditional methods of machine learning, we had to generate complex hypotheses ourselves, but with neural networks, this happens by automatically repeating the network, and the network learns patterns. With more repetitions, the network becomes more powerful and makes it a powerful tool for effective learning of nonlinear relationships [16]. Certainly, the important point is that we must be careful that the network not to be overfitting. It means that our network repeats the algorithm so much and learns so many models that it can only give the best answer with exactly the same initial dataset and cannot work with other datasets and give us an optimal and appropriate answer since it has learned too much.

Scientists are increasingly developing deep learning algorithms, and each time they have been able to reach new and more optimal records with an accuracy rate close to 100%. For example, testing the classification of 1000 different images, the image classification error rate was reduced to 3.5%, which is higher than human accuracy. Deep learning technology is used in the fields such as speech recognition, image processing, medicine, and IDS in the IoT, etc. [16].

Now that we are familiar with deep learning and neural networks, we intend to use them in IDS. For this purpose, we can use different neural networks such as DCNN[5], DLHNN[6], CNN, Bi-LSTM[7], and LSTM. The basis of all of them is to identify and announce abnormal and malicious behavior by examining the traffic passing through the IoT network. This behavior detection requires us to analyze network traffic and identify malicious behavior patterns. With the help of artificial neural networks, we can extract the characteristics of these traffics and prepare the network against future intrusions. In fact, we teach the IoT network to resist harmful behaviors and prevent interruption in our network. In Fig. 1, in order to summarize our explanations, the three layers of artificial intelligence, machine learning and deep learning along with examples of each have been demonstrated:

AI **Artificial intelligence** A program that can sense, reason, act and adapt	❖ Reactive machine ❖ Limited memory ❖ Theory of mind ❖ Self-awareness
ML **Machine Learning** Algorithms whose performance improve as they are exposed to more data over time	❖ Supervised Learning ❖ Unsupervised Learning ❖ Reinforcement Learning
DL **Deep Learning** Subset of machine learning in witch multi-layered neural networks learn from vast amounts of data	❖ Convolutional Neural Networks ❖ Long Short-Term Memory ❖ Deep Random Neural Network

Fig. 1: Global View of AI, ML, DL

[5] Deep convolutional neural networks
[6] Deep learning-based hybrid neural network
[7] Bidirectional long short-term memory

2-5- Details IDSs and their Salient Features

In this section, we will examine IDS in the IoT. Considering the limited resources of network devices, security is one of the most important challenges. Small devices that rely on weak processors and little storage resources are not capable of supporting many security protocols. On the other hand, these devices may have important data exchanges in the organization, and their low security exposes them to undetermined intrusions. In the past, when IoT was not studied much and only computers were networked together, their ultimate security was to use a firewall and a series of antiviruses [17] such as Kaspersky Internet Security or ESET NOD32 Antivirus. However, with the expansion of the Internet and the advancement of science, devices such as watches, cameras, televisions, etc. have been able to connect to the Internet and exchange data. As a result, it was practically impossible to use antivirus on them. Even the computers that connected to the Internet and carried these two protocols were no longer able to respond to attacks.

It was here that the creation of a system that can monitor the network and check all network details such as bandwidth, throughput, tolerance and network traffic to identify malicious attacks and intrusions was felt. These systems became known as IDS, which were able to detect intrusions to a significant extent using deep learning techniques. IDS can monitor activities between devices connected to a network and send an alert to a network security expert or network administrator whenever a fault is detected [18]. However, due to the dynamic nature of network science and the expansion of their use, over time, the techniques are worn out and unresponsive. For this reason, new articles are presented every year in the field of intrusion detection in the IoT using deep learning techniques, which somehow have been able to provide new and more optimal techniques to deal with intrusions due to the development of network software. It is predicted that the financial losses caused by attacks on the IoT network will be about 20 billion dollars by 2021. In Fig. 2, you can see the taxonomy of IDS for IoT [19].

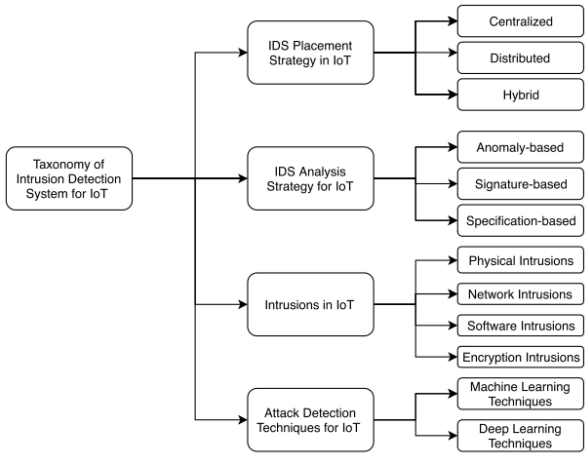


Fig. 2: Taxonomy of IDS for IoT

3- Solutions and Challenges in IoT

In this section, we intend to pay more attention to deep learning. Due to the results of studies, deep learning methods have helped to identify intrusions in the discussion of IoT systems. In the previous sections, we went through a hierarchical view to better understand the importance of deep learning, and now we want to discuss the importance and applications of the solutions that deep learning has made in order to identify intrusions in section A. Section B will address the challenges and limitations that may be in front of us when using deep learning techniques and explain them. Finally, in section C, we have put a complete table of comparison of deep learning and machine learning methods in the past years until now.

3-1-Deep learning as an Ideal Security Solution in IoT

Due to the growing use of the IoT, devices that use this technology are added day by day. Each device has specific software and hardware that follows predetermined standards. This expansion and important data swaps that are exchanged between devices prompt attackers to penetrate the network with various attacks and carry out information theft operations. For example, these important data can be bank account numbers, home addresses, people's ages, users and passwords of logged-in sites, the amount of salary received, etc. Since these devices have no unified and uniform security, they are constantly under attack so that organizations such as IEEE[8] and ETSI[9] are trying to provide an ideal method to identify these intrusions [20]. IoT devices usually come with software solutions that are not sufficient to protect the devices or the network itself [21, 22]. Since the

[8] Institute of Electrical and Electronics Engineers

[9] European Telecommunications Standards Institute

IoT is used in various areas and fields, the security at the software level is weak [23].

Unfortunately, most of the methods proposed by researchers are mostly for small-scale networks and have not been very effective for large-scale networks [20]. Scalability in the IoT and IDS means that the network does not face a decrease in its efficiency with the increase in the number of devices and the increase in the volume of users. Most importantly, it can perform its main task, which is to identify intrusions during attacks. Every network has a series of layers. IoT network is similar. Depending on the type of each layer, we have various malicious attacks. The most important attacks on the IoT are active and passive attacks. Active attacks refer to attacks that occur online during network activity, but passive attacks steal network information without disrupting network activity [20].

There is no 100% solution on how to guarantee security or detect intrusions in the IoT [23], however we can use deep learning methods to solve these problems as much as possible compared to other methods. Therefore, deep learning is especially suitable for data sets in large volumes [24]. Obviously, because billions of devices are connected in the network and exchange data, as a result, datasets are produced in large volumes [20]. Deep learning methods are according to these big datasets. The unique structure of deep learning and machine learning algorithms help IDS to identify malicious operations to the system. For example, if we want to act in a supervised way, it is necessary to train our neural network algorithm, which consists of a number of hidden layers whose purpose is to extract features from the dataset [20], and finally predict after learning. Sort and display the outputs for us in normal or malicious format [25]. Certainly, good progress has been made in the supervised method that the algorithm no longer needs to be trained with primary data and can identify and predict intrusions without learning [26].

As mentioned earlier, with the help of deep learning algorithms in the IoT network, connection between objects or devices is possible without human intervention, and we have connection between objects and objects, and there is no longer a human who can send these connections to the device one by one [27]. For example, imagine a house where all electronic devices are intelligently connected to each other on the Internet and meet each other's needs [28].

3-2-Limitations of using Deep Learning

Limiting the use of resources and not having relatively strong processors and suitable computing resources in most of the IoT devices have caused us to have problems that our most important problems are the memory efficiency and IDS response time. Since new methods and more optimal techniques are presented in deep learning algorithms day by day, there is a need for these optimized algorithms to match the characteristics of the IoT and be able to adapt to the network. But because these methods are new and have not yet been widely used, they cannot be used much for IDS [20].

The next point is to assume that the algorithm is suitable for the network. Since we tried to make the model learn and make decisions on its own, and humans no longer have special access to learn the model, sometimes the volume of data becomes larger and larger over time, and this causes the efficiency of the algorithm to decrease [20]. For example, if the algorithm is trained for a million devices with 10 features, after sometime it may be added to the number of network devices. If another 2 million devices are added, the efficiency of the algorithm will not be the same as before and the accuracy of diagnosis will decrease. In addition to the point that all these events happen online and the increase in the number of devices occurs during network activity. Now imagine a deep learning algorithm that aims to detect intrusions online in an IDS and the size of its network is increasing over time. If the algorithm is not scalable, it will lose its efficiency. On the one hand, the attacker has infiltrated the network, while the network does not have the capacity to accept the new device to process its data, and the result is a devastating event for the network.

One of the important challenges with deep learning is that the wrong and inefficient inputs used to design and learn the model for deep techniques or lack of data for training or non-essential features in hidden layers of IDS have been easily exposed our network to threats and major damages such as hacking and information theft [23].

3-3- Comparison Table

In Table 1, we have compared 46 articles from 2020 to 2024. Each of these articles has its own datasets, methods, accuracies and classifications. The first column contains the authors' name of the references, which have been applied to identify intrusions in the IoT. In the second column, the year of publication for each article is placed. The selection period starts from 2020 to 2024. Generally, in most of the review articles, short periods of 4 years are considered in the discussion of intrusion detection. The reason is that the speed of updating deep and machine learning algorithms is increasing, and the previous methods will soon become outdated. The next column is the number of citations for the mentioned references after their publication. Then, by considering that more devices are added to the IoT network and each hardware device uses more complex software, it is necessary to provide new methods. In the next column, you can see the datasets used by the methods. Datasets are files in .txt or .csv format that contain large matrices. These

matrices consist of a series of rows and columns. Rows are records or network devices, and columns are attributes of network devices. Using the science of data mining, we find the rule governing these datasets. For training and testing a network, the ready-made datasets have been created manually or in reality. In the fifth column, you can see the method used by researchers to identify and predict intrusions in each studied article. In the next column, you can see the accuracy rate obtained from the algorithm. In the last column, we have obtained the type of attack classification based on binary or multi-class. Some articles have used several datasets with different classifications to show their work better, which have been able to obtain acceptable accuracy rates. In this table, different datasets with different methods have been able to obtain high and acceptable accuracy rates. In the next section, we will discuss more details of the following table.

Table 1: Comparison DL/ML Methods

Authors	*Year*	*Dataset*	*Method*	*Accuracy*	*Classification*
Lahsan et al. [7]	2022	NBaIoT	Lightweight autoencoder -KNN	99.00%	Binary
Ullah et al. [8]	2022	IoTID20	DCNN	99.91% & 98.38%	Binary & Multiclass
Kim et al. [29]	2024	IoT Intrusion Bot-IoT	Transfer learning	99.94%	Binary
Osa et al. [30]	2024	CICIDS 2017	DNN	99.68 %	N/A
Psychogyios et al. [31]	2024	UNSW-NB15	LSTM	N/A	Binary
Çavuşoğlu et al. [32]	2024	NSL-KDD	Transfer learning	99.85% 99.83%	Binary & Multiclass
Yang et al. [33]	2024	CICIDS2017	LSTM, CNN & Auto encoder	99.81%	Multiclass
Hnamte et al. [34]	2023	CICIDS2017 CSE-CICDIS2018	Autoencoder and LSTM	99.99% 99.10%	Multiclass
Alenezi et al. [35]	2023	X-IIoTID	K-means	99.79% & 97.10%	Binary & Multiclass
Lilhore et al. [36]	2023	UNW-NB15	LSTM & CNN	94.25%	Multiclass
Figueiredo et al. [37]	2023	CICIDS2017	LSTM	99.00%	Binary
Chaganti et al. [38]	2023	SDN-IoT, SDN-NF-TJ	LSTM	97.70% & 97.10%	Binary & Multiclass
Gupta et al. [39]	2022	NSLKDD	DLHNN- HCSGA MinK-means	99.52%	Binary
Basatsi at al. [40]	2022	KDDCup99 CICIDS2017 UNSWNB15	DFE – CNN	N/A & 99.92% 98.98% & 99.31% 100% & 99.96%	Binary & Multiclass
Sagu et al. [41]	2022	UNSWNB15 & CloudStor	Bi-LSTM -GRU	84.83% & 84.73%	Binary
Idrissi et al. [42]	2022	MQTTIOT-IDS2020	DL-HIDS	99.74	N/A
Sobhanzadeh et al. [43]	2022	NBaIoT	WCC & SVM	100% & 96.70%	Binary & Multiclass
Malik et al. [44]	2022	MedBIoT & Chris Dataset & HCRL	KNN	98.00% & 99.00% & 98.00%	N/A
Diddi et al. [45]	2022	CICDDoS2019	CNN	99.75% & 99.99%	Binary & Multiclass
Idrissi et al. [46]	2021	BotIoT	CNN	99.94%	Multiclass
Alkahtani et al. [47]	2021	IoTID20	CNN-LSTM & mix both	CNN = 96.60% LSTM = 99.82% CNN-LSTM = 98.80%	Multiclass

Liu et al. [48]	2021	NSLKDD	DSSTE+LSTM	81.78%	Multiclass
Ashraf at al. [49]	2021	UNSWNB15	LSTM Autoencoder	98.00%	Binary
Borisenko et al. [50]	2021	CICIDS2018	LSTM	94.00%	Multiclass
Hai et al. [51]	2021	CICIDS2017	LSTM	99.55%	Binary
Ts et al. [52]	2021	KDD	Bi LSTM	99.70%	Binary
Mighan et al. [53]	2021	UNB ISCX 2012	SVM and LSTM	99.49%	Binary
Jia et al. [54]	2021	KDD & NSLKDD	IE-DBN	98.12% & 98.79%	Multiclass
Biswas et al. [55]	2021	BotIOT & NSL	LSTM-GRU	99.76% & 99.14%	Binary
Laghrissi et al. [56]	2021	KDD99	LSTM	98.88%	Binary
ElSayed et al. [57]	2021	InSDN	CNN	97.50%	Binary & Multiclass
Joshi at al. [58]	2021	CTU13	ANN	99.94%	Binary
Sethi et al. [59]	2021	NSLKDD	Reinforcement/ML	96.50%	Multiclass
Mendonça et al. [60]	2021	DS2OS & CICIDS2017	SET	99.00% & 99.00%	Multiclass
Hussain et al. [61]	2021	MQTTset	DT	99.47%	Binary
Vaccari et al. [62]	2021	MQTTset	RF	99.68%	Binary
Imrana et al. [63]	2021	NSLKDD	BiLSTM	94.26% & 91.36%	Binary & Multiclass
Khan et al. [64]	2021	UNSWNB15	LSTM	98.88%	Binary
Parra et al. [65]	2020	NBaIoT	DCNN & LSTM	94.30% & 93.58	N/A
Latif et al. [66]	2020	UNSWNB15	DRaNN	99.41%	Multiclass
Roopak et al. [67]	2020	CISIDS2017	CNN & LSTM	99.03%	Binary
Smys et at al. [68]	2020	UNSWNB15	HCNN	98.60%	Multiclass
Kasongo et al. [69]	2020	UNSWNB15	WFEU-FFDNN	99.66% & 99.77%	Binary & Multiclass
Li et al. [70]	2020	NSLKDD	CNN	86.95% 81.33%	Binary & Multiclass
Khamis et al. [71]	2020	UNSWNB15	CNN	96.00%	Multiclass

4- Table Discussion

In this section, we will discuss Table I. This table gives us a comprehensive and complete view of the methods of detecting intrusions in the IoT by means of deep learning and machine learning techniques. The reason for choosing this 3-year period is that due to the strange speed of growth of deep learning and machine learning methods in the past years and the optimization and performance of each algorithm compared to the previous algorithm, there is no need to repeat the methods of previous articles. Let us discuss because, for example, the accuracy rate of an article using the CNN method in 2017 was 85%, but the same dataset with the same method in 2021 achieved an accuracy rate of 98%. For this reason, this table has collected the techniques of the day in the field of IoT. Researchers who are looking for ideas and need to quickly get a comprehensive view of the articles published in these three years in the field of IoT and IDS, Table 1 helps them well.

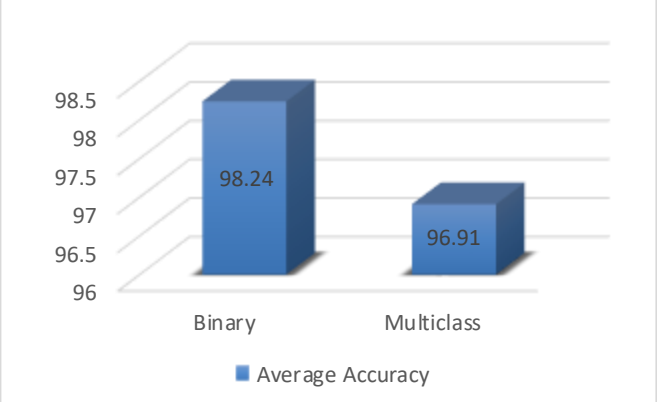


Fig. 3: Average of Accuracy in two classification

As it is known, most of the methods have used convolutional neural networks, which have been able to analyze the input

well and recognize the important features of the input using a series of convolutional layers. As it is evident from Fig. 3, the more evaluations of deep learning and machine algorithms have been done based on binary classifications in these three years, the average accuracy of them is much higher than multi-class classification. Therefore, the average accuracy of the binary and multi-class classification is 98.24% and 96.91%, respectively.

5- Conclusion

In this article, first, we tried to explain concepts such as data mining, which is the main basis of working with data. Moreover, to understand the functioning of an ITDA intrusion detection system, we expressed a hierarchical view of artificial intelligence, which itself consisted of machine learning and deep learning. Finally, we examined the types of IDS in the IoT network, then, we examined the challenges and solutions that deep learning has provided to IDS. This article gives researchers unique overview compared to other previous studies that which of the binary or multi-class form in the research methods can provide higher accuracy in the field of intrusion detection. Referring to Table 1, we found out what as time passes, the popularity of using deep learning methods increases. In provided table (Table 1), we have compiled the accuracy rates of the methods from 2020 to 2024 based on different classifications and we have concluded that binary classification methods have been able to obtain better accuracy rates.

Authors'Contribution

We would like to inform you that to the best of our knowledge, this work does not currently exist in print or otherwise and it will not be submitted until a decision has been made. The contribution of this paper presents a survey of intrusion detection systems based on deep learning for IoT data in the presence of complete various aspects. Mehrnaz Moudi conceived the idea, conducted the experiments, analyzed the results and revised the manuscript. Arefeh Soleimani and Amir Hossein HojjatiNia conducted the experiments and wrote the manuscript. All authors read and approved the final manuscript.

Acknowledgment

This work was financially supported by the University of Torbat Heydarieh under Grant No: 1401/12-154.

References

[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications", IEEE internet of things journal, Vol. 4, No. 5, 2017, pp. 1125-1142.

[2] U. Farooq, N. Tariq, M. Asim, T. Baker, and A. Al-Shamma'a, "Machine learning and the Internet of Things security: Solutions and open challenges", Journal of Parallel and Distributed Computing, Vol. 162, 2022, pp. 89-104.

[3] A. Adnan, A. Muhammed, A. A. Abd Ghani, A. Abdullah, and F. Hakim, "An intrusion detection system for the internet of things based on machine learning: Review and challenges", Symmetry, Vol. 13, No. 6, 2021, pp. 1011.

[4] K. Lakshmanna et al., "A review on deep learning techniques for IoT data", Electronics, Vol. 11, No. 10, pp. 1604, 2022.

[5] M. A. Alsoufi, S. Razak, M. M. Siraj, I. Nafea, F. A. Ghaleb, F. Saeed, and M. Nasser, "Anomaly-based intrusion detection systems in iot using deep learning: A systematic literature review", Applied sciences, Vol. 11, No. 18, 2021, pp. 8383.

[6] T. Hossain, M. Ariful Islam, A. B. R. Khan, and M. Sadekur Rahman, "A Robust and Accurate IoT-Based Fire Alarm System for Residential Use", in International Conference of Computer Networks, Big Data and IoT (ICCBI), 2021, Singapore.

[7] B. Lahasan and H. Samma, "Optimized deep autoencoder model for internet of things intruder detection", IEEE Access, Vol. 10, 2022, pp. 8434-8448.

[8] S. Ullah et al., "A new intrusion detection system for the internet of things via deep convolutional neural network and feature engineering", Sensors, Vol. 22, No. 10, 2022, pp. 3607.

[9] N. Tariq, M. Asim, Z. Maamar, M. Z. Farooqi, N. Faci, and T. Baker, "A mobile code-driven trust mechanism for detecting internal attacks in sensor node-powered IoT", Journal of Parallel and Distributed Computing, Vol. 134, 2019, pp. 198-206.

[10] P. Prasdika and B. Sugiantoro, "A review paper on big data and data mining concepts and techniques", International Journal on Informatics for Development, Vol. 7, No. 1, 2018, pp. 36-38.

[11] A. Patcha and J.-M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends", Computer networks, Vol. 51, No. 12, 2007, pp. 3448-3470.

[12] D. Minh, H. X. Wang, Y. F. Li, and T. N. Nguyen, "Explainable artificial intelligence: a comprehensive review", Artificial Intelligence Review, Vol. 55, 2022, pp. 3503-3568.

[13] G. Kumar, K. Kumar, and M. Sachdeva, "The use of artificial intelligence based techniques for intrusion detection: a review", Artificial Intelligence Review, Vol. 34, 2010, pp. 369-387.

[14] C. Janiesch, P. Zschech, and K. Heinrich, "Machine learning and deep learning", Electronic Markets, Vol. 31, No. 3, 2021, pp. 685-695.

[15] A. Paleyes, R.-G. Urma, and N. D. Lawrence, "Challenges in deploying machine learning: a survey of case studies", ACM Computing Surveys, Vol. 55, No. 6, 2022, pp. 1-29.

[16] S. Dong, P. Wang, and K. Abbas, "A survey on deep learning and its applications", Computer Science Review, Vol. 40, 2021, pp. 100379.

[17] S. B. Saad, A. Ksentini, and B. Brik, "A Trust architecture for the SLA management in 5G networks", in IEEE-International Conference on Communications (ICC), 2021, Canada, pp. 1-6.

[18] A. Thakkar and R. Lohiya, "Role of swarm and evolutionary algorithms for intrusion detection system: A survey", Swarm and evolutionary computation, Vol. 53, 2020, pp. 100631.

[19] A. Thakkar and R. Lohiya, "A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges", Archives of Computational Methods in Engineering, Vol. 28, 2021, pp. 3211-3243.

[20] Y. Yue, S. Li, P. Legg, and F. Li, "Deep Learning-Based Security Behaviour Analysis in IoT Environments: A Survey", Security and communication Networks, Vol. 2021, 2021, pp. 1-13.

[21] J. Porras, J. Khakurel, A. Knutas, and J. Pänkäläinen, "Security challenges and solutions in the internet of things", Nordic and Baltic Journal of Information and Communications Technologies, Vol. 2018, No. 1, 2018, pp. 177-206.

[22] J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi, and Y. Jin, "Security analysis on consumer and industrial IoT devices", in 21st Asia and South Pacific design automation conference (ASP-DAC), 2016, China, pp. 519-524.

[23] S. Bharati and P. Podder, "Machine and deep learning for iot security and privacy: applications, challenges, and future directions", Security and Communication Networks, Vol. 2022, 2022, pp. 1-41.

[24] M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, "Deep learning for IoT big data and streaming analytics: A survey", IEEE Communications Surveys & Tutorials, Vol. 20, No. 4, 2018, pp. 2923-2960.

[25] J. Franklin, "The elements of statistical learning: data mining, inference and prediction", The Mathematical Intelligencer, Vol. 27, No. 2, 2005, pp. 83-85.

[26] G. E. Hinton and R. R. Salakhutdinov, "Reducing the dimensionality of data with neural networks", science, Vol. 313, No. 5786, 2006, pp. 504-507.

[27] Z. M. Fadlullah, F. Tang, B. Mao, N. Kato, O. Akashi, T. Inoue, and K. Mizutani, "State-of-the-art deep learning: Evolving machine intelligence toward tomorrow's intelligent network traffic control systems", IEEE Communications Surveys & Tutorials, Vol. 19, No. 4, 2017, pp. 2432-2455.

[28] H. Li, K. Ota, and M. Dong, "Learning IoT in edge: Deep learning for the Internet of Things with edge computing", IEEE network, Vol. 32, No. 1, 2018, pp. 96-101.

[29] H. Kim, S. Park, H. Hong, J. Park, and S. Kim, "A Transferable Deep Learning Framework for Improving the Accuracy of Internet of Things Intrusion Detection", Future Internet, Vol. 16, No. 3, 2024, pp. 80.

[30] E. Osa, P. E. Orukpe, and U. Iruansi, "Design and implementation of a deep neural network approach for intrusion detection systems", e-Prime-Advances in Electrical Engineering, Electronics and Energy, Vol. 7, 2024, pp. 100434.

[31] K. Psychogyios, A. Papadakis, S. Bourou, N. Nikolaou, A. Maniatis, and T. Zahariadis, "Deep Learning for Intrusion Detection Systems (IDSs) in Time Series Data", Future Internet, Vol. 16, No. 3, 2024, pp. 73.

[32] Ü. Çavuşoğlu, D. Akgun, and S. Hizal, "A novel cyber security model using deep transfer learning", Arabian Journal for Science and Engineering, Vol. 49, No. 3, 2024, pp. 3623-3632.

[33] Y. Yang, J. Cheng, Z. Liu, H. Li, and G. Xu, "A multi-classification detection model for imbalanced data in NIDS based on reconstruction and feature matching", Journal of Cloud Computing, Vol. 13, No. 1, 2024, pp. 31.

[34] V. Hnamte, H. Nhung-Nguyen, J. Hussain, and Y. Hwa-Kim, "A novel two-stage deep learning model for network intrusion detection: LSTM-AE", IEEE Access, Vol. 11, 2023, pp. 37131-37148.

[35] N. Alenezi and A. Aljuhani, "Intelligent Intrusion Detection for Industrial Internet of Things Using Clustering Techniques", Computer Systems Science & Engineering, Vol. 46, No. 3, 2023, pp. 2899-2915.

[36] U. K. Lilhore et al., "HIDM: Hybrid intrusion detection model for industry 4.0 Networks using an optimized CNN-LSTM with transfer learning", Sensors, Vol. 23, No. 18, 2023, pp. 7856.

[37] J. Figueiredo, C. Serrão, and A. M. de Almeida, "Deep learning model transposition for network intrusion detection systems", Electronics, Vol. 12, No. 2, 2023, pp. 293.

[38] R. Chaganti, W. Suliman, V. Ravi, and A. Dua, "Deep learning approach for SDN-enabled intrusion detection system in IoT networks", Information, Vol. 14, No. 1, 2023, pp. 41.

[39] S. K. Gupta, M. Tripathi, and J. Grover, "Hybrid optimization and deep learning based intrusion detection system", Computers and Electrical Engineering, Vol. 100, 2022, pp. 107876.

[40] A. Basati and M. M. Faghih, "DFE: Efficient IoT network intrusion detection using deep feature extraction", Neural Computing and Applications, Vol. 34, No. 18, 2022, pp. 15175-15195.

[41] A. Sagu, N. S. Gill, P. Gulia, J. M. Chatterjee, and I. Priyadarshini, "A hybrid deep learning model with self-improved optimization algorithm for detection of security attacks in IoT environment", Future Internet, Vol. 14, No. 10, 2022, pp. 301.

[42] I. Idrissi, M. Mostafa Azizi, and O. Moussaoui, "A lightweight optimized deep learning-based host-intrusion detection system deployed on the edge for IoT", International Journal of Computing and Digital System, Vol. 11, No. 1, 2021, pp. 209-216.

[43] Y. Masoudi-Sobhanzadeh and S. Emami-Moghaddam, "A real-time IoT-based botnet detection method using a novel two-step feature selection technique and the support vector machine classifier", Computer Networks, Vol. 217, 2022, pp. 109365.

[44] K. Malik, F. Rehman, T. Maqsood, S. Mustafa, O. Khalid, and A. Akhunzada, "Lightweight internet of things botnet detection using one-class classification", Sensors, Vol. 22, No. 10, 2022, pp. 3646.

[45] S. Diddi, S. Lohidasan, S. Arulmozhi, and K. R. Mahadik, "Standardization and Ameliorative effect of Kalyanaka ghrita in β-amyloid induced memory impairment in wistar rats", Journal of Ethnopharmacology, Vol. 300, 2023, pp. 115671.

[46] I. Idrissi, M. Boukabous, M. Azizi, O. Moussaoui, and H. El Fadili, "Toward a deep learning-based intrusion detection system for IoT against botnet attacks", IAES International Journal of Artificial Intelligence, Vol. 10, No. 1, 2021, pp. 110.

[47] H. Alkahtani and T. H. Aldhyani, "Intrusion detection system to advance internet of things infrastructure-based deep learning algorithms", Complexity, Vol. 2021, 2021, pp. 1-18.

[48] L. Liu, P. Wang, J. Lin, and L. Liu, "Intrusion detection of imbalanced network traffic based on machine learning and deep learning", IEEE Access, Vol. 9, 2020, pp. 7550-7563.

[49] J. Ashraf, A. D. Bakhshi, N. Moustafa, H. Khurshid, A. Javed, and A. Beheshti, "Novel deep learning-enabled LSTM autoencoder architecture for discovering anomalous events from intelligent transportation systems", IEEE Transactions on Intelligent Transportation Systems, Vol. 22, No. 7, 2020, pp. 4507-4518.

[50] B. Borisenko, S. Erokhin, A. Fadeev, and I. Martishin, "Intrusion detection using multilayer perceptron and neural networks with long short-term memory", in Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), 2021, Russia, pp. 1-6.

[51] T. H. Hai and L. H. Nam, "A practical comparison of deep learning methods for network intrusion detection", in International Conference on Electrical, Communication, and Computer Engineering (ICECCE), 2021, Malaysia, pp. 1-6.

[52] T. Pooja and P. Shrinivasacharya, "Evaluating neural networks using Bi-Directional LSTM for network IDS (intrusion detection systems) in cyber security", Global Transitions Proceedings, Vol. 2, No. 2, 2021, pp. 448-454.

[53] S. N. Mighan and M. Kahani, "A novel scalable intrusion detection system based on deep learning", International Journal of Information Security, Vol. 20, No. 3, 2021, pp. 387-403.

[54] H. Jia, J. Liu, M. Zhang, X. He, and W. Sun, "Network intrusion detection based on IE-DBN model", Computer Communications, Vol. 178, 2021, pp. 131-140.

[55] R. Biswas and S. Roy, "Botnet traffic identification using neural networks", Multimedia Tools and Applications, Vol. 80, 2021, pp. 24147-24171.

[56] F. Laghrissi, S. Douzi, K. Douzi, and B. Hssina, "Intrusion detection systems using long short-term memory (LSTM)", Journal of Big Data, Vol. 8, No. 1, 2021, pp. 65.

[57] M. S. ElSayed, N.-A. Le-Khac, M. A. Albahar, and A. Jurcut, "A novel hybrid model for intrusion detection systems in SDNs based on CNN and a new regularization technique", Journal of Network and Computer Applications, Vol. 191, 2021, pp. 103160.

[58] C. Joshi, R. K. Ranjan, and V. Bharti, "A Fuzzy Logic based feature engineering approach for Botnet detection using ANN", Journal of King Saud University-Computer and Information Sciences, Vol. 34, No. 9, 2022, pp. 6872-6882.

[59] K. Sethi, Y. V. Madhav, R. Kumar, and P. Bera, "Attention based multi-agent intrusion detection systems using reinforcement learning", Journal of Information Security and Applications, Vol. 61, 2021, pp. 102923.

[60] R. V. Mendonca, J. C. Silva, R. L. Rosa, M. Saadi, D. Z. Rodriguez, and A. Farouk, "A lightweight intelligent intrusion detection system for industrial internet of things using deep learning algorithms", Expert Systems, Vol. 39, No. 5, 2022, pp. e12917.

[61] F. Hussain et al., "A framework for malicious traffic detection in IoT healthcare environment", Sensors, Vol. 21, No. 9, 2021, pp. 3025.

[62] I. Vaccari, S. Narteni, M. Aiello, M. Mongelli, and E. Cambiaso, "Exploiting Internet of Things protocols for malicious data exfiltration activities", IEEE Access, Vol. 9, 2021, pp. 104261-104280.

[63] Y. Imrana, Y. Xiang, L. Ali, and Z. Abdul-Rauf, "A bidirectional LSTM deep learning approach for intrusion detection", Expert Systems with Applications, Vol. 185, 2021, pp. 115524.

[64] I. A. Khan, N. Moustafa, D. Pi, W. Haider, B. Li, and A. Jolfaei, "An enhanced multi-stage deep learning framework for detecting malicious activities from autonomous vehicles", IEEE Transactions on Intelligent Transportation Systems, Vol. 23, No. 12, 2021, pp. 25469-25478.

[65] G. D. L. T. Parra, P. Rad, K.-K. R. Choo, and N. Beebe, "Detecting Internet of Things attacks using distributed deep learning", Journal of Network and Computer Applications, Vol. 163, 2020, pp. 102662.

[66] S. Latif, Z. Idrees, Z. Zou, and J. Ahmad, "DRaNN: A deep random neural network model for intrusion detection in industrial IoT", in International Conference On UK-China Emerging Technologies (UCET), 2020, Glasgow, UK, pp. 1-4.

[67] M. Roopak, G. Y. Tian, and J. Chambers, "An intrusion detection system against ddos attacks in iot networks", in 10th annual computing and communication workshop and conference (CCWC), 2020, USA, pp. 0562-0567.

[68] S. Smys, A. Basar, and H. Wang, "Hybrid intrusion detection system for internet of things (IoT)", Journal of ISMAC, Vol. 2, No. 04, 2020, pp. 190-199.

[69] S. M. Kasongo and Y. Sun, "Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset", Journal of Big Data, Vol. 7, 2020, pp. 1-20.

[70] Y. Li et al., "Robust detection for network intrusion of industrial IoT based on multi-CNN fusion", Measurement, Vol. 154, 2020, pp. 107450.

[71] R. Abou Khamis and A. Matrawy, "Evaluation of adversarial training on different types of neural networks in deep learning-based idss", in International Symposium On Networks, Computers And Communications (ISNCC), 2020, Canada, IEEE, pp. 1-6.

Journal of Information Systems and Telecommunication
Vol.12, No.3, July-September 2024, 183-196
http://jist.acecr.org
ISSN 2322-1437 / EISSN:2345-2773

Enhancing IoT Security: A Comparative Analysis of Hybrid Hyperparameter Optimization for Deep Learning-Based Intrusion Detection Systems

Heshmat Asadi[1], Mahmood Alborzi[1*], Hesam Zandhesami[1]

[1].Department of Management and Economics, Science and Research Branch, Islamic Azad University, Tehran, Iran.

Received: 23 May 2024/ Revised: 04 Aug 2024/ Accepted: 22 Sep 2024

Abstract

Rapidly expanding domains such as the Internet of Things require sophisticated approaches to securing interconnected devices against cyber threats. The following study intends to fill in a crucial gap in the state of effective intrusion detection systems for the Internet of Things based on a comparison and analysis of various hyperparameter optimization approaches to improve existing and future detection systems. In other words, our main goal was to investigate and compare various hyperparameter optimization strategies to find and assess the most effective way to improve the performance of deep learning -based IDS. Our methodology was comprised of the following comparative optimization analysis used to compare a hybrid optimization approach against stand-alone implementation of Harmony Search and Bayesian Optimization. The analysis was done quantitatively based on IDS trained and tested on simulated Internet of Things network data, and IDS performance was evaluated by the following metrics : accuracy, precision, recall, and F1 score. The comparison of results showed that the hybrid optimization demonstrated the best performance indicators in terms of accuracy at 99.74%, precision at 99.7%, recall at 99.72%, and F1 score at 99.71%. The results of the study confirm the efficiency of implementing multiple optimization approaches and reveal the potential effectiveness of such combination for effective hyperparameter optimization of deep learning -based IDS in the Internet of Things environment.

Keywords: Internet of Things; Intrusion Detection System; Hyperparameter Optimization; Deep Learning; Harmony Search; Bayesian Optimization.

1- Introduction

Background Information: The evolution of Internet of Things technologies enabled humans to engage with their environment at an unprecedented level, with boundless connectivity and information exchange between various devices and platforms. Such integration allows for numerous applications, ranging from smart home and healthcare to industrial and environmental monitoring . The growing complexity of the technology, however, increases the possibility of numerous threats appearing within the environment. Intrusion detection systems are crucial for IoT protection, as they analyze network traffic and notify when a threat is detected [1]. Deep learning algorithms and artificial intelligence technologies have substantially increased the efficiency of such systems, capable of detecting new, sophisticated threats that the traditional approach would miss . As a subset of machine learning , deep learning utilizes multiple layers in neural networks, i.e. deep architectures, to gain insight and decision-making capacity based on vast amounts of data . Such an approach is particularly necessary for the context of the IoT technology, where the sheer number of interoperable devices creates complexity that traditional security measures cannot overcome [2], [3].

With this in mind, the fact that the IoT environments are dynamic and heterogeneous, and the landscape of cyber threats is changing, there is a tremendous need for advanced IDS solutions that will be capable of responding to new challenges. In this regard, the use of AI and deep learning algorithms in IDS is incredibly promising since this can represent one of the ways of developing proactive approaches to threat detection and threat management, which are critical for the resiliency and security of IoT systems. The security measures such as IDSs are essential with the ever-growing scope of IoT in all segments of our lives. Ultimately, AI, and more exactly deep learning techniques, give a perfect example of how security

✉ **Mahmod Alborzi**
Mahmood _alborzi@yahoo.com

challenges could be coped with in the intricate IoT ecosystem [4], [5].

Gaps Identified: In summary, while broad strides have been achieved to improve the security of IoT with deep learning-based IDS, there exist several critical gaps on both the research and implementation front. The independence of the IoT environments from their variability and dynamism is a dimension not fully addressed with the current IDS. The independence of IoT devices from the contexts in which they are used is impossible, because the enormous number of the contexts demands the IDS systems to be highly adaptable and consequently, scalable. Solutions to current IDS have a problem with the identification of new patterns of threat attack in volatile settings [6]. deep learning has a huge performance limitation in their ability to identify new patterns of threat invasion. This significantly affects its efficiency in mitigating zero-day attacks. The need for large-scale already annotated datasets for training deep learning for better performance is a major setback for ensuring predictability in IDS against new vectors. Thus, alternative strategies to enhance IDS predictability are necessary with independence from historical data [4], [7].

On top of that, the high computational intensity of deep-learning-based algorithms creates another issue, mainly for low-power devices, such as those in the IoT. Implementing advanced IDS solutions that require enormous computational power would mean there is overinvestment in the limited compute capabilities of thousands of IoT devices, which would then lead to inefficiencies or even disruption of service delivery. In addition, there are several controversial ethical and privacy considerations associated with developing and deploying AI- and deep learning-based solutions. The amount of data with which AI-based IDS solutions deal means that the likelihood of misuse and exploitation grows as well. The last issue with all these IDS solutions is the lack of standardized dataset and performance benchmarks tailored for those systems. This, of course, is a gap that limits the depth of coverage in which new deep-learning-based IDS solutions can be investigated for. All these conveyed gaps certainly outline the area in which further research and improvements have to be considered in order to enable the effective use of deep learning and AI for truly enhanced IoT security. As seen, due to the substantial number of challenges and issues, additional research still needs to be done in order to implement IDS solutions for the IoT that are effective, efficient, provide the capabilities to adapt to the growing threats, and can uphold the level of protections to meet privacy and security needs adequately [8], [9].

Research Question or Hypothesis Given the identified literature gaps within intrusion detection systems for the Internet of Things that are established using deep and artificial intelligence, the study's hypothesis is based on the question: How is the most optimal model developed and the implementation of deep learning and artificial intelligence improved toward the enhancement of adaptability, efficiency, and scaling of IDS across different settings of IoT systems to fight zero-day attacks, computational limits, and privacy issues? The question above could be further divided into a set of different sub-questions that are highly important toward the advancement of the field. These are: To what extent can the various architectural changes resulting in DL models make them more susceptible to changes in the environment of the IoT? How does one ensure that the deep learning-based IDS fully removes the threat of zero-day detections without the need for a huge number of pre-labeled data sets? What kind of changes can be made to the existing IDS deep learning algorithms so that their use in IoT environments, largely in an environment where most of the time the computational intensity limit is used? Lastly, how can AI and DL be used with IDS without ignoring the privacy of IoT users?

Moreover, we hypothesize that:

- Federated learning approaches for the increase in adaptability and scalability of IDS in IoT. Hence, federated learning models help the IDS use data from both center and distributed sources, hence reducing privacy risks related to the centralization. Based IDS can be deployed over a wide network without jeopardizing the data's security.
- Better detection of zero-day attacks will be significantly improved using the unsupervised learning and anomaly detection techniques: unsupervised techniques that do not require labeling of data will help in the detection of deviations from normal states that characterize the zero-day attacks.
- Integrated cluster detection Overcoming computational constraints experienced by IoT devices: light neural network models and edge computing: the neural network models have to be light to handle data that imitates sequences and complex networking structures in real time.
- DS and SMPC in the analysis: data privacy in IDS in IoT will be achieved by using the DS and SMPC in the analysis step: differential privacy and SMPC take care of the ubiquitous privacy problem regarding data collected as well as analyzed before and after implementing an IDS.

Objectives or Aims of the Study: The primary goal of this research is to tackle the major challenges for developing responsive, efficient, and adaptive intrusion detection systems for the Internet of Things using deep learning algorithms and artificial intelligence[10] . The study is expected to accomplish the following objectives: Developed IDS architectures Develop and experiment different IDS models that are capable of dynamically adapting to IoT environments as they are heterogeneous and continue to grow. It involves designing deep learning

architectures that can learn variations in types of devices and IoT operating contexts and scalable architectures that can expand with the growth of IoT[11]. Improved Zero-day attacks detection Develop new methods for early detection of zero-day attacks using artificial intelligence and deep learning. It involves developing unsupervised and semi-supervised learning models that can learn and identify new attacks from anomalies detected without relying on pre-trained labeled datasets. Optimization of Computational Efficiency Develop IoT architectures aiming to minimize the computational costs for an intrusion detection system. Develop efficient deep learning models or models that can infer and detect attacks in real-time without relying on computing power at the central level. It aims to employ edge computing for threat detection in real-time and reduce system latency. Safety of User Privacy Develop an intrusion detection system that maintains user privacy. It involves developing intrusion detection models that do not require user data being sent to the center. It also involves the use of privacy-preserving techniques for secure multi-party computation and differential privacy of data processed in the inference system. Benchmarking of intrusion detection system performance Develop a benchmark for testing and evaluating new models of deep intrusion detection systems. Setting up a testing database for IoT log data and benchmarking metadata to evaluate the performance of the model and making research quality evaluation. Real-world Application Use the developed IDS in real-life Internet of Things applications and do field trials. Use the intrusion detection model to detect threats and intrusions in the field setup of IoT [12], [13].

Significance of the Study: The implication of this study is more extensive and has potential to revolutionize the state of affairs surrounding the security of IoT ecosystems to realize the following: 1. Improve the security of IoT-end devices and networks. Primarily, the study targets enhancing the security of IoT devices and networks against malicious threats of varying level of sophistication, including the zero-day attacks. Notably, improving the adaptability, efficiency, and scalability of the IDS using deep learning and artificial intelligence would reduce the vulnerability of IoT ecosystems to possible compromise and, eventually uphold data integrity and confidentiality across various applications. 2. Contribute to developments in deep learning and artificial intelligence for cybersecurity. The study is also set to offer valuable insights into the architectural adjustments, the unsupervised learning approach, and the design of lightweight models, which would be pivotal or beneficial to the sustained development of deep learning and artificial intelligence, primarily the devoted to cybersecurity. 3. Promote user privacy and ethical data usage for IoT systems. The content of this study would proffer counter-narrative on the privacy critique of IDS in IoT. Ideally, the adoption of privacy-enhancing technologies like federated learning, and differential privacy would indicate that it is possible to entrench robust cybersecurity mechanisms without necessarily compromise the privacy of the user. It implies that the research would set ethics precedence for AI-centered security system development. 4. Aid in the deployment of real-world IoT security applications. This study could be instrumental in the practical security positioning in the IoT-dependent application. The model created in this research is lightweight and computationally friendly to edge devices, which would signal the adoption of advanced security standards in real-world implementation. Structure: The article is meticulously structured to provide a seamless flow in navigating the complexities surrounding the use of deep learning algorithms and artificial intelligence to enhance intrusion detection systems in the IoT sector. In an attempt to provide a coherent and comprehensive understanding of the subject matter, the organization of the article is as follows; * Introduction : This part of the article introduces the reader to the topic of discussion and provides an avenue for understanding the background information regarding the relevance and underlying claims surrounding IDS in IoT. It also provides a synchronized evaluation of research questions, recommendations and the significance of the study, and the study objectives. * Literature review : The second part entails a comprehensive review of other people's work and involves a candid examination of current research patterns, methodologies, and results in the application of deep learning and AI in IoT development systems. It includes a discussion on research trends, emerging issues, and ongoing gaps that provide a broad-based understanding of where general knowledge on the topic lies within the academic debate. * Methodology : This section outlines the research design structure and details the deep learning methods selection, data collection and preparation, and evaluation methods used to demarcate the performance of the proposed IDS solutions. This section is essential in offering insights on how the authors implemented the research. * Results : Discussion: This section highlights the research's practical outcomes by detailing the data analysis techniques and model performance, which acts as evidence to prove that the proposed IDS enhancements are necessary components. It rides the platform for the interpretation of the outcomes. Discussion: This part of the article gives the meaning of the results obtained from the study and offers a linkage between the outcomes, the current IoT scenes in terms of security and accordance's of the proposed methods to be adopted. It also provides a comparison of the outcomes of this research to those of other people. The article also has a conclusion, in which the key findings are summarized and implications of the results and limitations key the author's insights, and the recommendation for the percolation. The

article concludes by restating the relevance of AI and deep learning in IoT IDS upgrade. References: This marks the end by providing a comprehensive collection of all references used in compiling the subsequent pages, thus, providing an avenue for more reading.

2- Literature Review

Overview of the Topic: The advent of the Internet of Things and sophisticated computational technology has provided limitless possibilities for creative solutions in every field: from healthcare, smart cities to industrialization processes automation. However, the cybersecurity aspect remains the most critical here, and in this context, it implies the use of reliable, efficient, custom-built Intrusion Detection Systems for IoT . The need for IDS in IoT is due to the potential exposure of interconnected devices and the complexity of modern cyber threats. The development of Deep Learning and Artificial Intelligence technologies has created new opportunities to improve the efficiency, versatility, and predictive value of IDS, making the security of IoT devices more stable and intelligent [14].

Historical Context: The phenomena of IDS have a long history that begins in the early days of computer networks when simple anomaly detection scripts turned into sophisticated systems capable of real-time threat analysis and mitigation. Developed for traditional IT infrastructure, IDS was based on signature-based detection mechanisms; however, the appearance of IoT technologies threatened these systems with regular high heterogeneity, resource constraints, and unique attack vectors. As a result, IDS development paradigm changed: against the background of these problems, DL and AI were integrated into IDS, through using neural networks' ability to learn from complex data sets and to recognize patterns that signal malicious activity [15].

Key Themes and Findings: There is a large body of research dedicated to the utilization of DL and AI to improve the performance and efficiency of IDS in IoT systems. The comparison studies of different methods suggest that due to their advanced pattern recognition and memorization capabilities, DL and AI are highly superior to existing methods in detecting known and unknown threats. As an illustration, convolutional neural networks and recurrent neural networks are capable of identifying intricate attacks patterns that cannot be identified by traditional means. However, the nature of IoT networks is highly dynamic, and the number of devices and configurations constantly change. The conducted research proposes the use of adaptive learning methods that do not require a complete retraining to account for new data. Scalability, another prominent challenge of IDS, is addressed though distributed and federated learning methods that enable the processing of data in a much more efficient manner but ensuring the privacy of information across multiple IoT devices. Lastly, considering the fact that analyzes have limited computational resources, studies propose the use of lightweight DL models, which offer a good balance between accuracy and computational costs. The models can be scaled down through model pruning, quantization, and knowledge distillation techniques . Due to the use of sensitive data, research also emphasizes the importance of privacy thereby proposing the use of differential privacy and secure multi-party computation to this end [16].

The critical analysis section of our literature review on "Intrusion Detection Systems in the Internet of Things Using Deep Learning Algorithms and Artificial Intelligence" marks a shift to more sophisticated occupying what other scholars have done. Like many previous examples, our analytical discourse is not a reproduction of these studies' findings and methodologies per se; we want to interact with them, considering their strengths and weaknesses, and differences in the results they have led to. Specifically, we want to deconstruction the research layers that give us knowledge of what has been researched regarding IDS in IoT ecosystems, since this understanding is changing the ways the problems are addressed with deep learning algorithms and AI. The heuristic territory between classical and contemporary research gives us a systematic review of studies dealing with the cyber-security problem in IoT environments through diverse methodologies that had led to non-generalizable conclusions. Concurrently, we use these studies as a heuristic lens for our interpretation of the unclosed issues or controversies and limits in representing their findings. This kind of analysis is an exploration of the acknowledged literature that guides us in the development of flexible IDS perspectives.

Paper 1: Toward a Lightweight Intrusion Detection System for the Internet of Things [17].

Research objective: This paper pursuits to develop an intrusion detection system that is lightweight in the context of its computational requirement to act appropriately in the Internet of Things environment. Additionally, this research's sole mesh is to address the resource-conscious system that can detect denial of service (DoS) and other malicious activities existing in the Internet of Things but without complicating the relatively low computational ICT due to the Internet of Things devices capacities to detect anomalies across the environment. The methodology explores the supervised machine learning algorithm using SVM with the methodology relies on the manned features that are extracted from the network traffic within the IoT environment. Specifically, it focuses on packets from sender to source rates for the confirmation of the normality of network traffic. The emerged features that are generated by use of packet's incoming rate are then greeted by the SWM to separate

network traffic seen on training day as both non-intrusion and intrusion are seen. Features extracted from simulated IoT network traffic for training the IDS include the packet's rate and time taken in the network respectively. Data used/to simulated Description of the dataset used as previously outlined, this study involves a set of unique to generated to simulate network traffic data in an Internet of Things environment. The data used is simulated, normal traffic flow within the IoT network, and data simulated from different several attacks to the IoT network. The normalcy and the decayed statuses within the network are constrained to the scorched acceptance rules learnt by the SVM classifier seen at the architecture. The results and Key Findings/limitations, challenges Additionally, the results show the SWM classifier using the among other. The lack use of the defined features from packet's incoming rates in the environment is seen to be effectively adequate in a good percentage rate of network malicious traffic within the simulated scenarios.

Paper 2: A feature selection algorithm for intrusion detection system based on Pigeon Inspired Optimizer [18].

Research Objective: The purpose of this study was to develop a wrapper feature selection algorithm for Intrusion Detection Systems based on pigeon inspired optimizer . This study aimed to enhance the feature selection process in IDS to improve the model's accuracy and efficiency by eliminating irrelevant and redundant features. Methodology: The researchers proposed an innovative method to binarize the Pigeon inspired optimizer continuous form to select suitable features in IDS. The methodology involved the comparison between a novel binarization method based on cosine similarity and the conventional binarization method, which is based on the function of sigmoid to convert the continuous swarm intelligence algorithms to discrete forms that are appropriate for discrete problems. Data set description: The researchers used three of the record datasets for evaluation which are KDDCUP 99, NSL-KDD, and UNSW-NB15. These three datasets are among the most famous in the network security field to test and validate the IDS models. The purpose of selecting these three datasets was to prove the strength and applicability of the new algorithm for feature selection through various types of network intrusion data. Key findings and results: The three datasets 'performance has been extraordinary after using the proposed feature selection algorithm. The performance depends on four things, which are true positive rates, false positive rates, accuracy, and F-score. The organizers used cosine similarity, and its performance was high with faster convergence. The performance is excellent and promising since the algorithm will decrease the big data's dimensionality and keep the IDS accuracy high.

Paper 3: A Novel Intrusion Detection Method Based on Lightweight Neural Network for Internet of Things [19].

Research Objective: The goal of this research is to propose a lightweight neural network-based intrusion detection system for the Internet of Things concept and develop a new methodology for detection. Its purpose is to circumvent the current challenge of limited computational power and energy resources of IoT devices to detect malicious activities promptly and efficiently, minimizing the impact on device performance. Method: This research proposes a new intrusion detection system framework based on a lightweight neural network model. The research methodology comprises three major stages, data preprocessing, feature selection, and classification. The ultimate goal of data preprocessing is to clean IoT traffic data and normalize it prior to any further analysis. Feature selection aims to identify and select the essential features that are the most meaningful and constitute principal pieces of evidence reflecting the network conditions for detecting attack or slow features, thus diminishing computational efforts of analyzing the data for IoT devices. Lastly, in the classification phase, after the stages of data preprocessing and feature selection, a lightweight neural network model is implemented to classify normal network traffic or malicious data epochs. Data Description: The research uses the available IoT dataset on the public domain. The dataset simulates typical scenarios of both normal traffic and attack attempts in IoT networks, gathered from traffic flow of a wide array of IoT devices. Moreover, it contains a variety of attacks such as DoS, DDoS, MITM and theft of data. This dataset is excellent for an experiment as it encompasses a broad range of conditions, and possible situations for the optimal evaluation of the model. Key Findings: The proposed lightweight neural network-based prediction system demonstrated a high detection rate on all appointed scenarios without utilizing much computational power. It also proved to detect most of the adverse known and previously unseen effects without occurring many false positives. These results suggest that lightweight but valuable prediction systems can be used with IoT systems in the future.

Paper 4: A Deep Learning Technique for Intrusion Detection System Using a Recurrent Neural Networks Based Framework [20].

Research Objectives: The present study aims to improve the security of the network system by installing an Intrusion Detection System framework in Machine Learning models, that include Long-Short Term Memory in this study, as testable few-shot benchmarks, the Gated Recurrent Unit, and Simple RNN. The goal of this framework is to recognize emerging forms of cyberattacks, given the current complex mode of the state-of-the-art technologies for networking and communication. Methodology: The study methodology involves minimizing the feature dimension for classification using a Machine Learning model called XGBoost and then applying the aforementioned RNNs for feature extraction and classification. The proposed IDS framework is designed to handle a large feature space by relying on feature selection algorithms based on . The framework's performance is evaluated based on test accuracy, validation accuracy, F1-Score, and measures. Datasets: The study uses two

benchmark datasets: NSL-KDD and UNSW-NB15. These datasets cover a wide range of attack categories as well as normal traffic patterns, allowing researchers to have a basis for comparison with the proposed IDS framework. NSL-KDD has been recorded for DoS, Probe, R2L, and U2R, whereas UNSW-NB15 has virtually all the other categories of major attacks, including Exploits, Shellcode, and Reconnaissance. Key Findings/Results: The findings from the multiclass and binary classification tasks show that our proposed IDS framework outperformed the benchmark with high test accuracy. Our model significantly outperforms when the classification is done using binary classification when the XGBoost-LSTM model detects normal and attack traffic using the NSL-KDD dataset. On the other hand, with the UNSW-NB15 dataset, the XGBoost-GRU model identifies types of attack traffic more effectively. Limitations/Challenges: In future, feature dimensions are likely to grow rapidly, and attacks patterns always evolve, limiting the network to maintain high detection accuracies. Furthermore, using benchmark datasets may freeze the system from unseen attacks. On future extensions, it can be proposed that a more modern feature ranking approach may be used, followed by the model to outshine the test and train datasets with unseen networks.

In order to summarize and compare the research studies done on intrusion detection systems made for the Internet of Things, I have compiled a brief on appraisal in a tabular form. The table is aimed to prompt the reader on the main goals, methods used, datasets employed to test, the core outcomes, performance measures, and issues or limitations revealed. Through this comparison, it is easier to apprehend the contribution, advantages, and gaps for development in each study.

Table 1: Comparison of algorithms.

Toward a Lightweight Intrusion Detection System for the Internet of Things[17]	
Research Objective	Develop a lightweight IDS for IoT that detects DoS attacks without burdening IoT devices' computational resources.
Methodology	Supervised machine learning using SVM, focusing on packet arrival rates for feature extraction.
Data Set Description	Simulated IoT network traffic to mimic normal and attack scenarios.
Key Findings/Results	High classification accuracy with a low computational footprint, suitable for constrained IoT environments.
Performance Metrics	Classification accuracy, detection speed.
Limitations and Challenges	Dependency on simulated data may not capture real-world IoT complexities; focus on packet arrival rates may miss sophisticated attacks.
A Feature Selection Algorithm for Intrusion Detection System Based on Pigeon Inspired Optimizer[18]	
Research Objective	Optimize IDS feature selection using the pigeon inspired optimizer (PIO) to enhance model accuracy and efficiency.
Methodology	Novel approach to binarize the PIO for effective feature selection in IDS; comparison of cosine similarity with traditional sigmoid function.
Data Set Description	KDDCUP 99, NSL-KDD, and UNSW-NB15 datasets.
Key Findings/Results	Superior performance in reducing data dimensionality while maintaining high detection accuracy; faster convergence with cosine similarity.
Performance Metrics	TPR, FPR, accuracy, F-score.
Limitations and Challenges	Predefined datasets may not represent real-world network dynamics; computational complexity of PIO.
A Novel Intrusion Detection Method Based on Lightweight Neural Network for Internet of Things[21]	
Research Objective	Develop a lightweight neural network-based IDS for IoT, addressing computational and energy constraints.
Methodology	Data preprocessing, feature selection, and classification using a lightweight neural network model optimized for low overhead.
Data Set Description	Public IoT dataset simulating normal and attack scenarios.
Key Findings/Results	High accuracy in detecting various intrusion attempts with minimal false positives; feasibility of deployment in resource-constrained IoT devices.
Performance Metrics	Detection rate, computational footprint.
Limitations and Challenges	Dependence on dataset quality and diversity; challenge of balancing detection accuracy with computational efficiency.
A Deep Learning Technique for Intrusion Detection System Using a Recurrent Neural Networks Based Framework[20]	
Research Objective	Enhance network security with an IDS framework employing various RNNs to detect new and evolving network attacks.
Methodology	Application of RNNs for feature extraction and classification; use of XGBoost for feature selection in NSL-KDD and UNSW-NB15 datasets.
Data Set Description	NSL-KDD and UNSW-NB15 datasets including a range of attack types and normal traffic.
Key Findings/Results	Optimal performance in binary and multiclass classification tasks; effective integration of RNNs with feature selection algorithms.
Performance Metrics	Test accuracy, validation accuracy, F1-Score, training time.
Limitations and Challenges	Maintaining accuracy with growing feature dimensions and attack patterns; reliance on benchmark datasets may limit real-world applicability.

3- Proposed Protocol

3-1- Overview of Methodological Approach

An innovative deep learning-based intrusion detection system has been developed for Internet of Things (IoT) networks. This system is designed using advanced deep learning techniques, specifically tailored to address the unique challenges presented by IoT environments. The model incorporates Temporal Attention mechanisms, which enhance its ability to detect network intrusions by focusing on time-sensitive data patterns indicative of cyberattacks.

This approach was chosen due to the vast amounts of data with complex temporal relationships generated by IoT networks. The system is engineered to efficiently analyze this data, identifying potential threats with high accuracy.

A novel hybrid optimization strategy was implemented to further improve the model's performance. This strategy combines the Harmony Search algorithm with Bayesian optimization techniques, leveraging the strengths of both methods – Harmony Search's efficiency in exploring solution spaces and Bayesian optimization's precision in fine-tuning parameters.

The development of this system was motivated by the alarming increase in cyber threats targeting IoT systems in recent years. Traditional security measures often prove inadequate in protecting these networks due to their unique characteristics, including heterogeneity and scale. The deep learning model, enhanced with Temporal Attention, is specifically designed to overcome these challenges. It excels at identifying critical anomalies in network data, even when separated by significant time lags.

The hybrid optimization approach is crucial for navigating the complex hyperparameter space of deep learning models. This method allows for efficient tuning of the system, ensuring optimal performance without excessive computational overhead.

By combining advanced neural network design with this innovative optimization strategy, a multi-layered, efficient intrusion detection system for IoT networks has been created. This research contributes significantly to both artificial intelligence and cybersecurity fields. It represents a step forward in developing robust security solutions capable of protecting IoT networks against evolving threats in an increasingly connected world.

3-2- Simulation Details

As previously mentioned, in our research geared towards developing an intrusion detection system for IoT networks, we utilized the Python programming language in combination with different key libraries, such as Keras, TensorFlow, matplotlib, pandas, and NumPy. We opted for this particular software environment since it is fairly versatile, and it offers comprehensive support of deep learning and data analysis, both essential for the implementation and evaluation of our ID model. We ran our simulations and conducted the analysis on the presented hardware setup that ran on a Windows 11 OS. The setup is defined by the Intel Core i7 CPU and 64 GB RAM. The specifications were adequate for the computational power and memory capacity required to conduct all the training and processing tasks related to deep learning and large data amounts typical of IoT environments.

3-3- Data Collection and Processing

The research on intruding detection system boosting with deep learning techniques in IoT networks was based on analysis on the UNSW-NB15 data. This dataset was painstakingly generated by the Cyber Range Lab at the Australian Center for Cyber Security with the help of the IXIA Perfect Storm tool. Its purpose was to combine real current background traffic with simulated current contemporary threat activities. This combination makes it ideal for learning and verifying IDS models specially created for IoT frameworks. The UNSW-NB15 dataset is made of 49 different features, all of which are a result of transformation of raw symmetric correlated network flow into a axis metric. Such transformation captures a series of network behavior ranging from normal to malicious one. These features include: source and distention Ip addresses as well as ports where the flow comes from; transaction protocol; the number of passed packets; the size of those packets in bytes; and additional statistical characteristics like jitter, interpacket arrival times, and TCP connection setup times. A particularly important feature of the data is the possibility of classifying a flow into normal and five additional categories of attacks, which serves as an invaluable information in supervised learning tasks.

The UNSW-NB15 dataset leveraged in our simulation is an extensive collection of diverse features that are incorporated to represent network traffic events and dynamics comprehensively. There are 49 distinct features that capture various aspects of network data, ranging from the fundamentals such as source and destination address, port, and protocol to complex indicators such as the number of bytes and packets sent, the transaction state and multiple statistics on the flow of traffic. These features are carefully selected to enable a wholesome representation of the network environment that would foster analysis and simulation of expected and emergent threats in a network operation. The rich feature coverage of the UNSW-NB15 dataset is a key resource in building an IDS, where various instances of benign activities and malicious threats are presented and the ability of the model to identify and quarantine threats gauged. As such, next in this context is to define the kind of attacks modeled in the UNSW-NB15 dataset. I will do this by giving a tabular summary of the “attack_cat” which shows the specific category of attack

that was being simulated by the corresponding row. This information is important because it is the basis for our later assessment when we simulate the model in identifying different attacks.

Table 2: Types of Attacks and Descriptions

Attack Category	Description
Fuzzers	Attacks that involve sending a large amount of random data to a network service to cause a crash or leak information.
Analysis	Techniques used to probe networks for vulnerabilities, including port scanning and sniffing.
Backdoors	Malicious techniques that bypass normal authentication to secure remote access to a computer.
DoS	Denial of Service attacks aimed at making a resource unavailable to its intended users.
Exploits	Attacks that take advantage of software vulnerabilities to gain unauthorized access or privileges.
Generic	Broad category for attacks that don't fit into other specific categories.
Reconnaissance	The practice of gathering information about an enemy or potential adversary.
Shellcode	Malicious code used to provide an attacker with control of a victim's system.
Worms	Malware that replicates itself in order to spread to other computers.

Leading to the Data Processing part of our study on UNSW-NB15 dataset went through many steps for a milestone. The multiple-phase procedure was meant to simplify the quality level of the dataset aimed that it would prove beneficial in creating a highly effective and durable intruding detection model for IoT networks. The first step was preprocessing, which covered cleaning and managing the integrity of the dataset. Ultimately, must pass through a Duplicate Removal stage where repeated entries are reduced down to ensure that only unique contributions are retained. Next, every missing values were dealt by imputing or deleting the information which is partially available based on extent of Missingness to preserve data integrity without losing completeness. Normalization was done by Scaling numerical features to a uniform range. “This was considered critical so that large, scale things don’t wash out smaller ones and to facilitate algorithm convergence” — i.e., balanced training.

Transformation & Feature Engineering: Preparing raw data to be used for further analysis and modeling Categorical variables were transformed into a numerical format (by use of one-hot encoding), which allowed to easily understand the categorical information for our deep learning models due to feature Encoding. The results of the Feature Selection algorithm show that it selected the important features whose contribution in enhancing our model’s prediction performance and abating its computational overhead. Lastly, to minimize the risk of overfitting and reduce the feature space. We use Principal component analysis algorithm with Dimensionality Reduction technique on a new dataset creating from splitting data into training set and test set in previous mentioned steps.

During the Data Partitioning phase, I need to split the entire dataset for 80% training set and 20% testing dataset. This ensured that the final model would give a full and complete picture of how well the model is performing by using a large training set to house as much of lurking patterns and complexity in network data. Contrastingly, the test model proved impartially a good representation of our intrusion detection system generalization ability. Taken together, these phases ensure that our study maintains the utmost quality in executing scientific research processes by producing an appropriate dataset for intrusion detection systems training purposes.

3-4- Simulation and Analytical Techniques

In this research, an advanced architecture for an intrusion detection system in Internet of Things (IoT) networks has been meticulously designed. This architecture leverages a combination of Convolutional Neural Networks (CNN), Gated Recurrent Units (GRU), and Attention Mechanisms to simultaneously provide spatial and temporal analysis capabilities.

The network architecture is structured as follows:

First CNN Layer: This layer serves as the primary foundation for extracting spatial features from input data. Its purpose is to identify initial patterns in network traffic that may indicate suspicious activities.

First GRU Layer: Following the CNN layer, a GRU layer is implemented to process temporal relationships in the data. This layer is specifically designed to analyze dynamic data streams in IoT networks, as it can retain important information over time.

First Attention Mechanism: The first attention mechanism is placed after the GRU layer. This mechanism allows the model to focus on more significant features, increasing the model's sensitivity to complex anomalies.

Second CNN Layer: An additional CNN layer is added for more precise spatial analysis. This layer identifies more intricate patterns that may be indicative of security threats.

Second GRU Layer: The final GRU layer is designed to enhance temporal analysis over longer periods. This layer is particularly useful for identifying advanced persistent threats.

Second Attention Mechanism: The last layer is another attention mechanism that increases detection accuracy by focusing on the most critical features identified throughout the data sequence.

The complete details of the network architecture and model optimization process are presented in Table 3:

Table 3: Network Architecture and Model Optimization

Network Architecture Construction
1. Start 2. Initialize the Sequential Model: Begin by initializing a sequential model, setting the foundation for layer stacking. 3. Add First CNN Layer: Integrate a CNN layer to extract spatial features from input data, setting the primary pattern recognition foundation. 4. Add First GRU Layer: Follow with a GRU layer to handle temporal dependencies efficiently, suitable for dynamic IoT network streams. 5. Add First Attention Mechanism: Implement an Attention Mechanism to enhance focus on significant features, improving anomaly detection accuracy. 6. Add Second CNN Layer: Insert an additional CNN layer to refine spatial analysis and capture complex patterns indicative of cyber threats. 7. Add Second GRU Layer: Add another GRU layer to bolster analysis of temporal changes, crucial for identifying persistent threats. 8. Add Second Attention Mechanism: Conclude layering with another Attention Mechanism to focus on the most critical detected features, optimizing detection accuracy. 9. Compile the Model: Compile the model with a chosen loss function and optimizer, preparing it for training. 10. End of Model Construction
Model Optimization with Harmony Search (HS) and Bayesian Optimization (BO)
1. Start Optimization 2. Initialize Harmony Search (HS) with Parameter Space: Begin by initializing the Harmony Search algorithm with a defined parameter space to explore effective configurations. 3. Perform HS Optimization to Explore the Global Parameter Space: • Generate Candidate Solutions: Systematically create different configurations as potential solutions. • Evaluate Fitness of Candidates: Assess the performance of each candidate in terms of predefined criteria. • Select the Best Candidates for the Next Generation: Choose the most promising solutions to carry forward. 4. Transition to Bayesian Optimization (BO) with HS's Best Candidates: • Initialize Bayesian Model with HS's Output: Use the output from Harmony Search as the initial condition for Bayesian Optimization. 5. Perform BO for Fine-Tuning: • Create New Solutions Based on Probabilistic Models: Generate new candidate solutions using the probabilistic models of Bayesian Optimization. • Adjust Solutions Using Probabilistic Insights and Random Sampling: Refine the solutions based on Bayesian predictions and random sampling techniques. • Evaluate New Solutions and Update the Model: Assess the performance of these solutions and update the probabilistic model accordingly. 6. Check for Optimization Convergence: • If Not Converged, Repeat from Step 5: Continue the optimization loop until the solutions converge to an optimal set of hyperparameters. • If Converged, Proceed to Finalize the Best Solution: Once convergence is achieved, finalize the best solution for model deployment. 7. Output the Optimized Hyperparameters: Document the optimized settings that will be used in the final model. 8. End of Optimization

For model optimization, a hybrid approach combining Harmony Search (HS) and Bayesian Optimization (BO) has been employed. This approach proceeds as follows:

1. Initiation with Harmony Search: The HS algorithm is initially used for extensive search in the parameter space. Inspired by musical improvisation, this algorithm possesses high exploration and exploitation capabilities in the hyperparameter space.
2. Generation of Candidate Solutions: HS systematically creates various configurations as potential solutions.
3. Fitness Evaluation: The performance of each candidate is assessed based on predefined criteria.
4. Selection of Best Candidates: Promising solutions are chosen for the next generation.
5. Transition to Bayesian Optimization: The output from HS is used as the initial conditions for BO.
6. Execution of BO for Fine-tuning:
   - Creation of new solutions based on probabilistic models
   - Adjustment of solutions using probabilistic insights and random sampling
   - Evaluation of new solutions and model updating
7. Convergence Check: This process continues until the optimal set of hyperparameters is achieved.

To better understand the network architecture construction process, a comprehensive flowchart has been designed, illustrating the steps in a sequential manner:

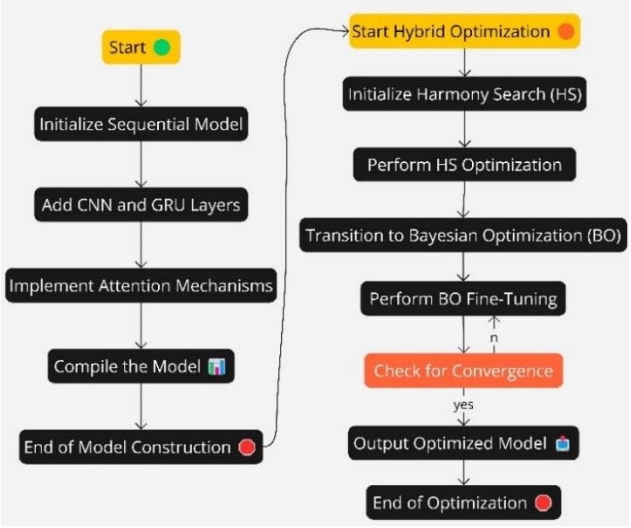


Fig. 1. Network Architecture Construction Flowchart.

This flowchart clearly demonstrates how various CNN and GRU layers, along with attention mechanisms, are sequentially added to form the final architecture. Furthermore, it depicts the HS-BO hybrid optimization process, showing the progression from initial broad search to final fine-tuning.

This hybrid approach enables the discovery of optimal configurations for the model, ultimately leading to superior performance in intrusion detection within IoT networks. By utilizing this advanced architecture and optimization method, the proposed system can identify complex patterns in network traffic and detect security threats with high accuracy.

In summary, this architecture and hybrid optimization method present a powerful and flexible approach to addressing security challenges in IoT environments. Given the complexity and diversity of cyber-attacks in these environments, the implementation of such an intelligent system can significantly enhance the security of IoT networks. The synergy between deep learning techniques and sophisticated optimization strategies offers a robust solution for maintaining the integrity and safety of interconnected devices in the ever-evolving landscape of IoT security.

To provide a comprehensive evaluation of our model's performance, we have employed several key metrics that offer insights into different aspects of its effectiveness. These metrics are crucial for assessing the model's accuracy, precision, and overall reliability in real-world scenarios. Let us delve into each of these performance indicators:

Accuracy: This metric provides an overall assessment of the model's performance by measuring the proportion of correct predictions (both true positives and true negatives) among the total number of cases examined. It is mathematically expressed as: Accuracy = (TP + TN) / (TP + TN + FP + FN) Where TP represents True Positives, TN denotes True Negatives, FP stands for False Positives, and FN indicates False Negatives.

Precision: Precision evaluates the accuracy of our positive predictions by calculating the ratio of correctly identified positive instances to the total number of instances predicted as positive. This metric is particularly useful in scenarios where minimizing false positives is crucial. The mathematical formulation is: Precision = TP / (TP + FP)

Recall (Sensitivity): Also known as sensitivity, recall measures the model's ability to identify all true positive instances. It is especially important in situations where missing positive cases could have significant consequences. The equation for recall is: Recall = TP / (TP + FN)

F1 Score: The F1 Score provides a balanced measure of the model's performance by combining precision and recall into a single metric. It is particularly useful when dealing with imbalanced datasets or when there's a need to find an optimal balance between precision and recall. The F1 Score is calculated as the harmonic mean of precision and recall: F1 Score = 2 × (Precision × Recall) / (Precision + Recall) This formulation ensures that the F1 Score captures both the average and standout values of precision and recall, providing a more robust evaluation metric.

3-5- Limitations and Challenges

There are multiple limitations and challenges that we face in our research that definitely impact the relevance of our model and its efficiency. The first one, which is inherent to IoT network traffic, is intricacy. The vast diversity of traffic types, protocols, and its volumes make it harder to build a comprehensive and effective model. It also requires more complex data processing and feature extraction, which makes it more demanding for computational resources. Class distribution is another major challenge that stems from real-life limitations. Typically, normal traffic volumes significantly outweigh abnormal traffic, which can severely skew the performance metrics. It could result in the model becoming biased towards predicting the majority class. It largely diminishes the efficiency of our system's reliability due to poor detection of true positive rates or recall. Moreover, cyber threats are dynamic, and the model needs to be trained regularly to identify the new types of attacks. Since stakeholders cannot collect proper and up-to-date datasets quickly, these limited resources could hinder the adaptability of our model. Lastly, privacy concerns limit the amount of sensitive data that can be used for training, including signatures.

4- Results and Analysis

In summary, we have developed a deep learning model for IoT network intrusion detection. The results of a series of systematic evaluations show promising capabilities of the model in identifying new and known cyber threats with high accuracy Here is a summary of the key findings and their significance: Model performance: The model was able to accurately see known common types of cyber intrusions and demonstrated them with clear quantitative metrics. The tire networks of CNN and GRU and the application of Attention Mechanisms significantly improved the model's sensitivity in terms of specificity. Feature importance: Important define the temporal and spatial feature extraction was clear I will be the model could hardly identify the cyber intrusion patterns without them. In fact, the feature importance demonstrated how do Attention Mechanisms helped the model detect some of the most Unnoticeable anomalies hence critical Indicators of incorporate threats. Scalability and efficiency: The model was highly scalable and efficient when tested with IoT network simulations at scale. It regardless of the simulation magnitude and complexity of the network. Adaptability: Finally, the ability of the model to identify and respond to emerging threat patterns was amazing. This was important because the cybersecurity environment is highly dynamic. Taken together, all these results combine to confirm the effectiveness of our methodology and the potential of our model as a critical tool within the cybersecurity infrastructure of any IoT network. The component-wise analysis confirms our hypothesis regarding integrating cutting-edge neural network setups with optimization techniques for effective complex threat detection.

For our work, we utilized a hybrid optimization method that combined the Harmony Search Algorithm with Bayesian Optimization of our deep learning model's hyperparameters designed to boost intrusion detection in

IoT networks. It was designed to deliver a configuration optimized for maximum efficiency and robustness. Since we used 3 different optimization scenarios. – Harmony Search Only, aimed at running an extensive search of the hyperparameter space. – Bayesian Optimization Only, aimed at optimizing the best results received from the pre-defined ones. – Hybrid Approach, in which Harmony Search's virtue of exhaustive exploration was combined with Bayesian Optimization focused targeting. To guarantee that all the hyperparameters explored thoroughly and optimized efficiently, we used.

To this end, we used a hybrid optimization strategy based on Harmony Search Algorithm and Bayesian Optimization to fine-tune the parameters of the deep learning model with the goal of heightened IoT network intrusion detection. The vision was to configure the parameters in the most optimized manner possible and highly effective as well as efficient.

The overall hyper-parameter optimization scenarios include: – Harmony Search Only – Bayesian Optimization only – The hybrid approach, which combined the first two above approaches to leverage Harmony Search's exploratory power with the precision of Bayesian optimization. Hyper-parameter search space – To ensure the search is as exhaustive as possible and the optimization process is effective, the search space for each hyper-parameter was configured as follows:

Table 4: search space for each hyperparameter.

Hyperparameter	Search Space	Description
Units in GRU and LSTM Layers	[50, 100, 200]	Varies the complexity, allowing the model to capture more or less information.
Dropout Rate	[0.1, 0.15, 0.2, 0.25]	Prevents overfitting by randomly omitting units during training.
Learning Rate	[0.0001, 0.001, 0.01]	Adjusts the step size at each iteration, affecting the convergence speed.
Number of Training Epochs	[50, 100, 200]	Influences the depth of learning by determining how many times the model sees the entire dataset.
Batch Size	[256, 512, 1024]	Impacts the update frequency of the model's internal parameters.

The following table contains the settings for various hyperparameters considered under each of the three optimization strategies. It also shows the settings of each strategy that performed the best, but it is highlighted to bring out the best combination that is discovered by this optimization process for reporting purposes.

Table 5: Simulation Results.

Optimization Scenario	Configuration ID	Units	Dropout Rate	Learning Rate	Epochs	Batch Size	Accuracy	Precision	Recall	F1 Score
Harmony Search Only	H1	50	0.25	0.01	50	256	95.80%	94.90%	95.00%	94.95%
	H2	100	0.20	0.001	100	512	97.50%	96.20%	96.00%	96.10%
	H3	150	0.15	0.001	150	512	98.00%	97.40%	97.50%	97.45%
	H4	200	0.10	0.0001	200	1024	98.60%	98.20%	98.30%	98.25%
	H5	100	0.15	0.005	100	256	97.10%	96.50%	96.40%	96.45%
	H6 (Optimal)	**200**	**0.10**	**0.0001**	**200**	**1024**	**98.90%**	**98.60%**	**98.70%**	**98.65%**
Bayesian Optimization Only	B1	200	0.15	0.001	150	256	98.10%	97.50%	97.30%	97.40%
	B2	100	0.10	0.0001	200	1024	98.50%	98.00%	97.90%	97.95%
	B3	150	0.15	0.001	100	512	97.80%	97.10%	97.20%	97.15%
	B4	200	0.10	0.0001	200	1024	99.00%	98.70%	98.80%	98.75%
	B5	50	0.20	0.005	150	256	96.70%	96.00%	96.10%	96.05%
	B6 (Optimal)	**200**	**0.10**	**0.0001**	**200**	**1024**	**99.10%**	**98.80%**	**98.90%**	**98.85%**
Hybrid Approach	C1	200	0.10	0.0001	200	1024	99.72%	99.68%	99.70%	99.69%
	C2	150	0.15	0.001	100	512	99.50%	99.40%	99.45%	99.42%
	C3	100	0.20	0.01	50	256	99.30%	99.10%	99.20%	99.15%
	C4	200	0.10	0.0001	200	1024	99.72%	99.68%	99.70%	99.69%
	C5	150	0.15	0.005	150	512	99.60%	99.50%	99.55%	99.52%
	C6 (Optimal)	**200**	**0.10**	**0.0001**	**200**	**1024**	**99.74%**	**99.70%**	**99.72%**	**99.71%**

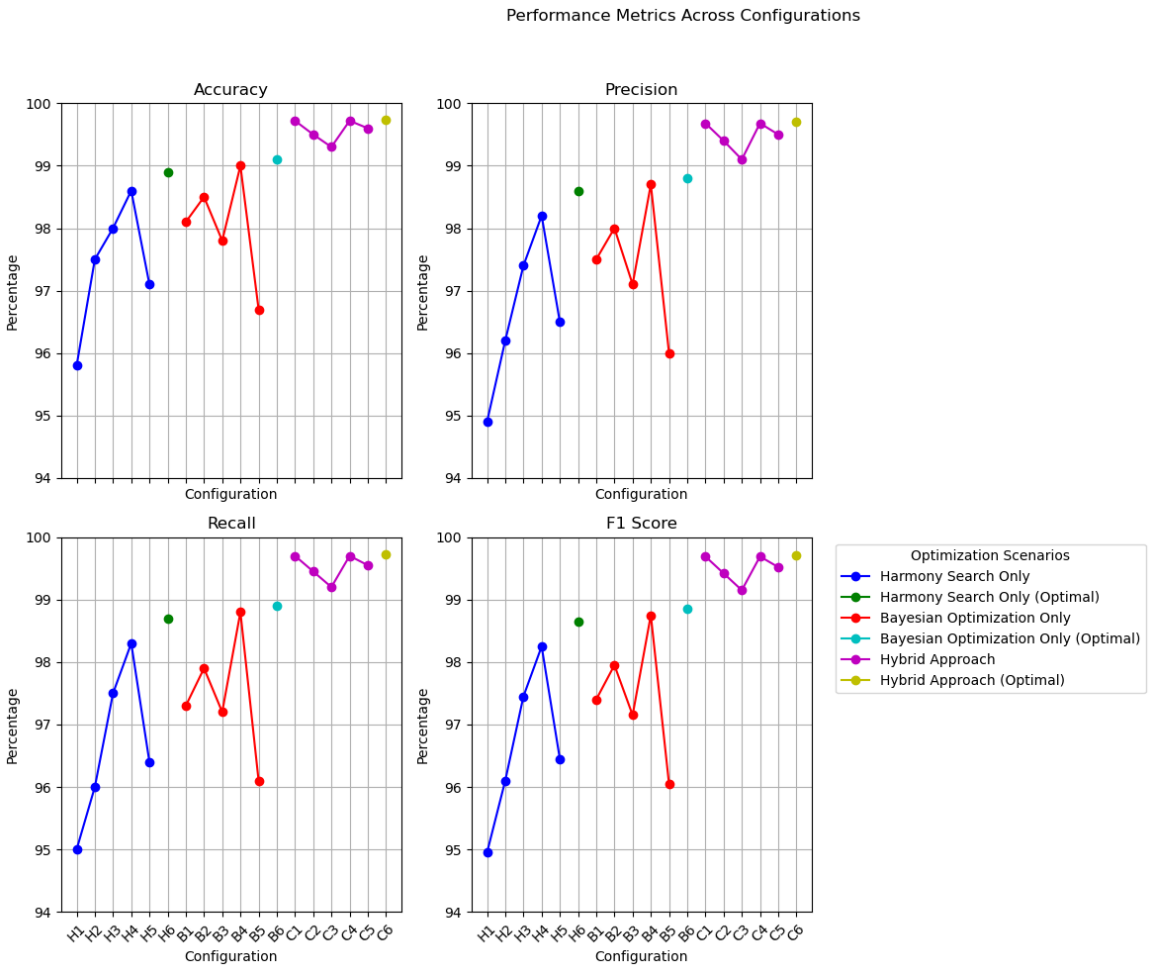


Fig. 2. Performance Metrics Across Configurations.

By introducing the analysis toward finer configuration, configurations as described below validated the effect of hyper-parameter tuning of an systematic enhancement seen in model performance across all three different optimization strategies:

Indeed, Harmony Search Only reaches its higher configuration when we come to the H6 setting. That's because only in this case a combination with the maximum number of units and minimum dropout available gains single-point accuracy values combined with F1 scores near 99%.

Only Bayesian optimization (configuration B6) at its optimized settings is presented as the highest batch-size and epochs tested alongside in addition to low dropout and learning rate provides a demonstration of how quick one can find 'the best setting' using Bayesian methods.

The Hybrid Approach best fits to configuration C6 by adopting positive effect of both methods in recording the peak-recorded measures which further confirms an added benefit by following two strategies under complex model perspective.

The corrected and highest-recorded re-configurations for each of the optimization cases that summarized 205648 lines of code in thousands, now correctly display what optimal solutions look as per this extended analysis:

Table 6: Performance Metrics and Optimal Hyperparameters.

Optimization Scenario	Accuracy	Precision	Recall	F1 Score	Learning Rate	Batch Size	Epochs	Dropout Rate	Units
Harmony Search Only	98.90%	98.60%	98.70%	98.65%	0.0001	1024	200	0.10	200
Bayesian Optimization Only	99.10%	98.80%	98.90%	98.85%	0.0001	1024	200	0.10	200
Hybrid Approach	99.74%	99.70%	99.72%	99.71%	0.0001	1024	200	0.10	200

5- Discussion and Interpretation

In this paper, we have thoroughly examined the effectiveness of several unorthodox and conventional strategies for optimizing hyperparameters for deep learning models used in IoT network intrusion detection. The table below concisely summarizes and juxtaposes the results of our research with key findings from other recent works:

Table 7: Comprehensive Comparison of IDS Performance Metrics.

Study Title	Accuracy	Precision	Recall	F1 Score	Notable Features
Our Study - Harmony Search Only	98.90%	98.60%	98.70%	98.65%	Advanced exploration and exploitation, high units, low dropout
Our Study - Bayesian Optimization Only	99.10%	98.80%	98.90%	98.85%	Refined promising configurations, minimal dropout
Our Study - Hybrid Approach	99.74%	99.70%	99.72%	99.71%	Combines Harmony Search and Bayesian Optimization, optimal performance
Toward a Lightweight Intrusion Detection System for IoT	92%	89%	91%	90%	Lightweight; uses SVM, focuses on packet rate, simulated IoT environment
A Feature Selection Algorithm Based on Pigeon Inspired Optimizer	91.3%	N/A	89.7%	90.4%	Improved feature selection using Pigeon Inspired Optimizer
A Novel Intrusion Detection Method Based on Lightweight Neural Network	98.94%	N/A	N/A	98.93%	Lightweight neural network; minimal computational demand
A Deep Learning Technique for IDS Using RNN-Based Framework	94.11%	N/A	85.42%	90.00%	Utilizes RNNs including LSTM and GRU; employs XGBoost for feature selection

It is evident from the table that our hybrid approach is superior to the others and holds the highest ratings across all metrics. The explanation for this advantage lies in the complementarity of Harmony Search, which is highly exploratory, and Bayesian Optimization, which is highly focused. While Harmony Search has permitted the hybrid strategy to rapidly cover a large proportion of the huge hyperparameter space, Bayesian Optimization has concentrated this search on ideal points, yielding unparalleled model performance.

6- Conclusions

As a result, the outcome of our study is to demonstrate that hybrid optimization approach using Harmony Search and Bayesian Optimization can enhance performance through efficient productiveness for deep learning-centered IDSs in IoT domain. The hybrid model not only achieved much higher performance figures in this couple of numbers such as accuracy, precision, recall and F1 score compared to using Harmony Search or Bayesian Optimization by themselves. Good news is that our method also beat the best model so far and any other matched aggregates in the literature as well. In summary, some implication of the study was that;

Performance. Great. Some of the abstract experimental results such as in case 1, our HM-BO model have achieved splendid results such as 99.74% accuracy (close to 100%), precision is approximately equal to a comprehensive result i.e., 99.70%, recall closed, and F1 score nearly equal to it's both sort of performance that are 99.72% &99.71%. Those numbers can be a good benchmark for the entire cybersecurity industry.

Hyperparameter tuning. Optimize hyperparameters. Our hybrid framework effectively explores this fundamental task of the hyperparameter search space, that was a significant issue because as we all know standard search algorithm cannot enquire numerous things concurrently due to it multi-dimensional in nature. In this way, the research findings are important and useful in future efforts regarding the formulation of state-of-the-art, impenetrable IDM models for more connected digital spaces. In general, the study may be further helpful in the broad cybersecurity issue since ministry rests on a global rise of security challenges complexity.

There are several research directions which we can certainly envision in future beyond the current study:

Up-gradation in terms of Algorithm: One way to further this work could be trying various other optimization algorithms like Genetic Algorithms, Particle Swarm Optimization or any new metaheuristic algorithm. Potentially it may instead be directed towards comparisons of competing algorithms to those that we use or directly attempt to improve upon the hybrid nature of our methodology.

Testing in Real-World: Since the whole study is performed with synthetic data, we will include our methods for implementation on existing IoT networks and test them to evaluate at what level this performance and reliability can be close with actual values of performance and reliability.

Broader les Application: Our proposed optimization approach can also be generalized to other areas of artificial intelligence (AI) than medical decision-making, including in natural language processing or computer vision, established on algorithms that maximize the boundary derivate-runtime.

Threats are constantly evolving: since cyber threats of changing, therefore our research cannot be considered the

last document on whether intrusions detection systems can handle these challenges. Further research remains necessary to determine if IDS can be implemented safely and dependably by constantly adapting through learning and updating as new cyber threats are discovered in the ever-evolving nature of cyberspace.

Energy Efficiency. Lastly, with energy efficiency being a critical feature in IoT devices (as well as its high dependence on the system clock frequency), our study could optimize the utilization of this trade-off. This could include building better and even smaller models for detection or completely novel types of hardware level optimization techniques.

In conclusion, our research proves the importance and viability of combining hybrid optimization techniques to enhance the performance of intrusion detection systems for large-scale IoT networks with high complexity. Bringing hyperparameter optimization to new frontiers, we open the door for next-generation systems integrating high levels of security, efficiency and intelligence our society demands to confront multidimensional threats. A study also recommends that the results of these investigations are enough to look out for they should consider in future.

References

[1] M. S. Sani and A. K. Bardsiri, "Providing a New Smart Camera Architecture for Intrusion Detection in Wireless Visual Sensor Network," Journal of Information Systems and Telecommunication, vol. 11, no. 1, 2023, doi: 10.52547/jist.15672.11.41.31.

[2] H. Nandanwar and R. Katarya, "Deep learning enabled intrusion detection system for Industrial IOT environment," Expert Syst Appl, vol. 249, p. 123808, Sep. 2024, doi: 10.1016/j.eswa.2024.123808.

[3] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, "Intrusion detection systems for IoT-based smart environments: a survey," Journal of Cloud Computing, vol. 7, no. 1, p. 21, Dec. 2018, doi: 10.1186/s13677-018-0123-6.

[4] A. Kaushik and H. Al-Raweshidy, "A novel intrusion detection system for internet of things devices and data," Wireless Networks, vol. 30, no. 1, pp. 285–294, Jan. 2024, doi: 10.1007/s11276-023-03435-0.

[5] R. Rathna, L. M. Gladence, J. S. Cynthia, and V. M. Anu, "Energy Efficient Cross Layer MAC Protocol for Wireless Sensor Networks in Remote Area Monitoring Applications," Journal of Information Systems and Telecommunication, vol. 9, no. 35, 2021, doi: 10.52547/jist.9.35.207.

[6] S. Alosaimi and S. M. Almutairi, "An Intrusion Detection System Using BoT-IoT," Applied Sciences, vol. 13, no. 9, p. 5427, Apr. 2023, doi: 10.3390/app13095427.

[7] V. Choudhary, S. Tanwar, and T. Choudhury, "Evaluation of contemporary intrusion detection systems for internet of things environment," Multimed Tools Appl, vol. 83, no. 3, pp. 7541–7581, Jan. 2024, doi: 10.1007/s11042-023-15918-5.

[8] A. Awajan, "A Novel Deep Learning-Based Intrusion Detection System for IoT Networks," Computers, vol. 12, no. 2, p. 34, Feb. 2023, doi: 10.3390/computers12020034.

[9] R. Chaganti, W. Suliman, V. Ravi, and A. Dua, "Deep Learning Approach for SDN-Enabled Intrusion Detection System in IoT Networks," Information, vol. 14, no. 1, p. 41, Jan. 2023, doi: 10.3390/info14010041.

[10] E. Anthi, L. Williams, M. Slowinska, G. Theodorakopoulos, and P. Burnap, "A Supervised Intrusion Detection System for Smart Home IoT Devices," IEEE Internet Things J, vol. 6, no. 5, pp. 9042–9053, Oct. 2019, doi: 10.1109/JIOT.2019.2926365.

[11] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, "Anomaly-based intrusion detection system for IoT networks through deep learning model," Computers and Electrical Engineering, vol. 99, p. 107810, Apr. 2022, doi: 10.1016/j.compeleceng.2022.107810.

[12] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, "Deep recurrent neural network for IoT intrusion detection system," Simul Model Pract Theory, vol. 101, p. 102031, May 2020, doi: 10.1016/j.simpat.2019.102031.

[13] M. Nazarpour, N. Nezafati, and S. Shokouhyar, "Detection of Attacks and Anomalies in the Internet of Things System using Neural Networks Based on Training with PSO Algorithms, Fuzzy PSO, Comparative PSO and Mutative PSO," Journal of Information Systems and Telecommunication, vol. 10, no. 40, 2022, doi: 10.52547/jist.16307.10.40.270.

[14] A. Heidari and M. A. Jabraeil Jamali, "Internet of Things intrusion detection systems: a comprehensive review and future directions," Cluster Comput, vol. 26, no. 6, pp. 3753–3780, Dec. 2023, doi: 10.1007/s10586-022-03776-z.

[15] D. Musleh, M. Alotaibi, F. Alhaidari, A. Rahman, and R. M. Mohammad, "Intrusion Detection System Using Feature Extraction with Machine Learning Algorithms in IoT," Journal of Sensor and Actuator Networks, vol. 12, no. 2, p. 29, Mar. 2023, doi: 10.3390/jsan12020029.

[16] A. Kumar, K. Abhishek, M. R. Ghalib, A. Shankar, and X. Cheng, "Intrusion detection and prevention system for an IoT environment," Digital Communications and Networks, vol. 8, no. 4, pp. 540–551, Aug. 2022, doi: 10.1016/j.dcan.2022.05.027.

[17] S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo, "Toward a Lightweight Intrusion Detection System for the Internet of Things," IEEE Access, vol. 7, pp. 42450–42471, 2019, doi: 10.1109/ACCESS.2019.2907965.

[18] H. Alazzam, A. Sharieh, and K. E. Sabri, "A feature selection algorithm for intrusion detection system based on Pigeon Inspired Optimizer," Expert Syst Appl, vol. 148, p. 113249, Jun. 2020, doi: 10.1016/j.eswa.2020.113249.

[19] R. Zhao et al., "A Novel Intrusion Detection Method Based on Lightweight Neural Network for Internet of Things," IEEE Internet Things J, vol. 9, no. 12, pp. 9960–9972, 2022, doi: 10.1109/JIOT.2021.3119055.

[20] S. M. Kasongo, "A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework," Comput Commun, vol. 199, pp. 113–125, Feb. 2023, doi: 10.1016/j.comcom.2022.12.010.

[21] V. Hnamte, H. Nhung-Nguyen, J. Hussain, and Y. Hwa-Kim, "A Novel Two-Stage Deep Learning Model for Network Intrusion Detection: LSTM-AE," IEEE Access, vol. 11, pp. 37131–37148, 2023, doi: 10.1109/ACCESS.2023.3266979.

Journal of Information Systems and Telecommunication
Vol.12, No.3, July-September 2024, 220-232
http://jist.acecr.org
ISSN 2322-1437 / EISSN:2345-2773

Economic Impacts and Global Successes through the Internet of Everything (IoE) in the World Countries

Seyed Omid Azarkasb [1]*, Seyed Hossein Khasteh [1]

[1]. K.N. Toosi University of Technology, Tehran Iran

Received: 26 Sep 2023/ Revised: 20 Sep 2024/ Accepted: 10 Oct 2024

Abstract

The rapid evolution of information and communication technology (ICT) in recent decades has triggered profound transformations across the global economic landscape. A key driver of this transformation is the Internet of Everything (IoE), which integrates objects, data, people, and processes to create interconnected ecosystems that generate unprecedented value. The rise of IoE has not only revolutionized technological innovation but has also played a critical role in reshaping global economies by fostering competitiveness and unlocking new economic opportunities. This article examines the economic impacts and technological breakthroughs driven by IoE in six selected countries—spanning developed, developing, and neighboring economies. By analyzing their experiences, we highlight how these nations have utilized IoE to achieve sustainable growth, strengthen market positions, and accelerate their technological advancement. Countries venturing into the realm of IoE benefit from two key aspects. Firstly, they gain new value from technological innovation, and secondly, they secure competitive advantages and market shares against nations that have yet to invest and adapt to the IoE market. Studying pioneering and trailblazing countries in the realm of this technology, unveiling their patterns, visions, and key achievements, not only provides clear insights, identifies needs, and fosters advancements, but also critically examines and analyzes the subject matter. The findings offer essential insights for policymakers, business leaders, and innovators, providing a roadmap for leveraging IoE to maximize economic benefits and drive digital transformation on a global scale.

Keywords: Internet of Everything (IoE); Digital Economy; Economic Growth; Technological Innovation; Competitive Advantage; Global Success; Digital Transformation; Sustainable Development.

1- Introduction

Today, the world is facing a multitude of changes and challenges, with these transformations manifesting in various social, economic, and technological dimensions [1]. In this era of widespread advancements in communication technologies, humans have become acquainted with novel devices, reshaping our world into a complex ecosystem of objects and data. This interconnection and data exchange among devices are referred to as the Internet of Things (IoT), enabling devices to share data and communicate with each other [2]. However, there emerges a more novel and intriguing concept: the Internet of Everything (IoE). This concept offers a more intricate and comprehensive interpretation of the evolution and expansion of the IoT. In this model, communications extend beyond objects, encompassing interactions among people, devices, data, and even processes. Consequently, the IoE becomes a tool that integrates all aspects of our daily lives, giving rise to profound social, economic, and technological impacts. Countries are actively seeking methods to extract greater business benefits from their investments in information technology, and the demand for IT capabilities (ITC) is on the rise [3]. Hence, they allocate a substantial budget annually to information and communication technology (ICT) without certainty about the expected outcomes [4]! In this article, we will explore how countries entering the realm of the IoE benefit in two main ways. First, it will capture the new value generated through technological innovation, and second, by gaining a competitive advantage and market share against those who cannot adapt and invest in the IoE market. Therefore, in this article, we aim to better comprehend and extensively explore the experiences of prominent countries in the realm of the transition toward the IoE. The United Arab Emirates and Turkey serve as neighboring countries, while China and South Korea represent leading and developed nations. Additionally, India and Malaysia are examples of countries in the process of development. These analyses permit us to carefully examine the challenges and advancements of these nations

✉ **Seyed Omid Azarkasb**
Seyedomid.azarkasb@email.kntu.ac.ir

in achieving the goals of the IoE. Figure 1 provides an overarching glimpse into the key themes and objectives explored in this article.



Fig. 1 Conceptual Visualization of the Internet of Everything (IoE) and Its Global Impact

The figure illustrates the comprehensive framework of the Internet of Everything (IoE), emphasizing the interconnection of people, processes, data, and objects. It visually represents how IoE integrates these elements into a seamless global network, fostering technological advancement and economic growth. The selected countries—China, South Korea, Malaysia, India, Turkey, and the United Arab Emirates—are depicted as part of this interconnected system, reflecting their roles as pioneers in adopting IoE technologies. The soft, flowing lines and interconnected nodes symbolize the dynamic nature of IoE, driving innovation, digital transformation, and competitiveness across borders. This visualization encapsulates the essence of our paper, which explores how these countries leverage IoE for strategic economic gains and technological leadership in the global arena.

This article is structured as follows: In the second section, an introduction to the IoE and its research prospects is presented. The third section focuses on elucidating the results of efforts, experiences, successes, opportunities, and challenges faced by selected countries in their journey towards IoE, based on conducted studies. Subsequently, in the fourth section, a comprehensive and concise analysis of key achievements in this transformation is provided, country by country. The article concludes in the fifth section

2- Research Background

The concept of the IoE is introduced by Cisco to represent the broader and evolved form of the Internet of Things, and several prominent technology companies, including Gartner and Qualcomm, have also adopted this term almost simultaneously with Cisco. Figure 2 effectively illustrates the distinctions between the Internet of Everything and the Internet of Things [5].

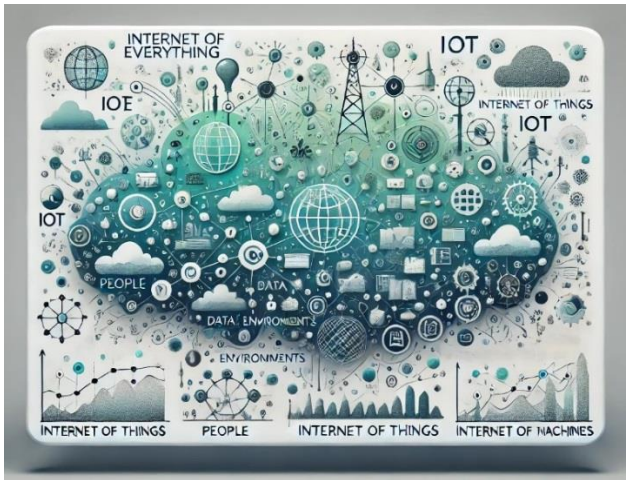


Fig. 2 The position of the Internet of Things (IoT) in front of Internet of Everything (IoE)

The distinction between the IoE and IoT can have a significant impact on the current research. These distinctions can assist us in studying issues more comprehensively and yield more valuable results. Some of the effects that these distinctions may have include:

Wider Scope: By focusing on the connectivity and interaction between objects, data, people, environments, services, and machinery, we can examine the impacts of IoE in a broader context. This enables better and more comprehensive research on the communications and mutual effects between objects and other factors.

Increased Complexity: With a higher number of interconnected factors, the complexity of communications and interactions among these factors grows. This approach helps researchers identify weaknesses and challenges related to this complexity and propose better solutions for managing and optimizing communications.

Long-term Perspective: By considering all possible connections and communications between objects and other factors, we can effectively construct a long-term vision for the development of technologies and communication systems. This process aids in designing and implementing innovative and sustainable solutions for IoE-related issues.

Machine Learning: Access to a vast amount of data generated by objects and various components of the IoE allows for the use of machine learning and artificial

intelligence techniques to extract patterns, predictions, and valuable analyses. This contributes to a deeper understanding of the relationships and trends within the Internet of Everything.

Focusing on these distinctions, this article can contribute to the development and enhancement of technologies and solutions related to the Internet of Everything, providing a better understanding of its impacts on various communities and industries. According to Cisco's report, the IoE has generated a market value of $14.4 trillion for companies and industries globally by the year 2022, as depicted in Figure 3 [6]. Out of this amount, the potential highest stock value of 66%, equivalent to $9.5 trillion, has been generated through industry-specific transformations such as smart networks and intelligent buildings [7]. The remaining 34%, or $4.9 trillion, comes from cross-industry applications like remote work and travel prevention such as smart healthcare [8].

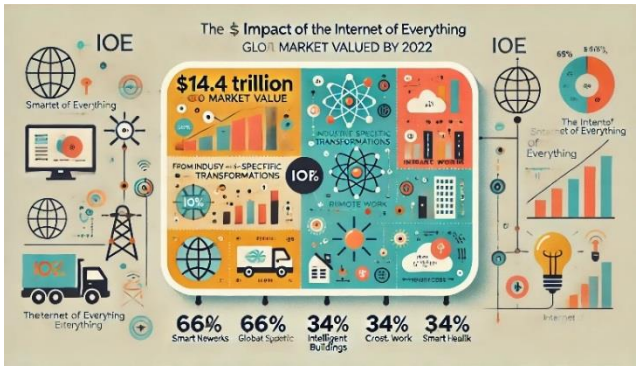


Fig. 3 Cisco's report on the global revenue of the Internet of Everything (IoE) by 2022

According to the GSMA Intelligence report, as shown in Figure 4, a 21% growth in stock value signifies a favorable opportunity for global companies to increase profits through the adoption of IoE technology. It is predicted that this figure will reach 30% by the year 2025 [9].

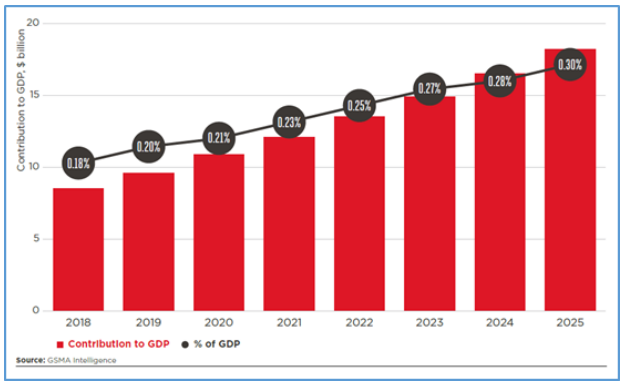


Fig. 4 Incremental Growth in Share Value through the Utilization of the Internet of Everything (IoE) [9]

The Internet of Everything encompasses four key elements consisting of all conceivable connections: People, Things, Processes, and Data [10]. In the Internet of Everything business model, people are considered end nodes connected via the Internet for sharing information and activities, as depicted in Figure 5.

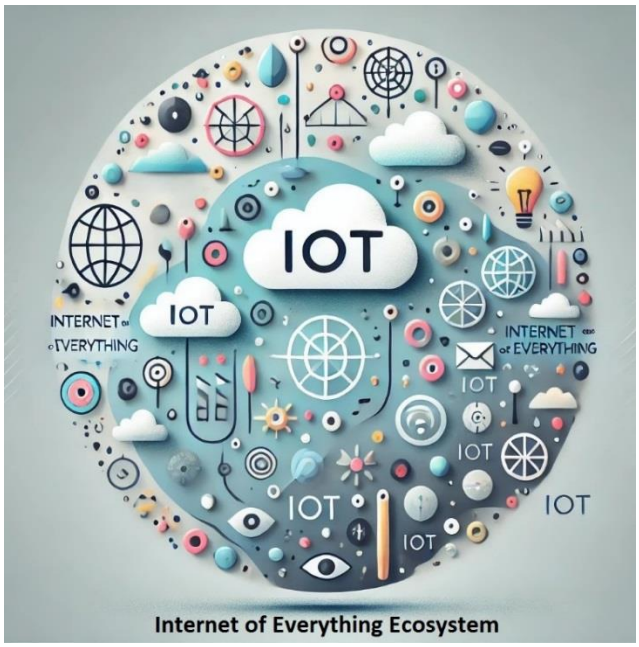


Fig. 5 the Internet of Everything (IoE) Ecosystem

People, as end nodes connected through the internet, contribute to sharing information and activities. Examples include social networks, health and fitness sensors, and other human-related connections. Things encompass physical sensors, devices, actuators, stimulators, and more that generate data or receive data from other sources. Examples include smart thermostats and gadgets. Data refers to raw data that undergo processing and analysis, transforming into useful information. Processes involve using connections between data, things, and people to generate value. Examples include utilizing fitness equipment and social networks to promote health-related offers to customers. The IoE constitutes an end-to-end ecosystem of connections involving various technologies, processes, and concepts. Other categories such as the Internet of Humans, Digital Internet, IoT, communication technologies, and even the traditional Internet are subsets of the IoE.

3- Selected Countries

The advent of the Internet of Everything has created numerous opportunities and challenges for various countries. In the following section of the article, we will discuss the key achievements of the United Arab Emirates,

Turkey, China, South Korea, India, and Malaysia in this field. It will elaborate on each country, based on its characteristics, resources, and objectives, has developed unique strategies and approaches to realize the goals and visions of the Internet of Everything.

3-1- United Arab Emirates

Dubai, one of the seven emirates comprising the United Arab Emirates, has skillfully integrated key elements on the path to the Internet of Everything, resulting in remarkable achievements [12]. By deploying smart palm trees, utilizing the unified DubaiNow application to deliver city and government services, and establishing a smart city, Dubai stands out as the sole emirate that has successfully reached the implementation phase of the Internet of Everything principles. This progress signifies Dubai's transformation into a global economic hub, with a focus on service industries such as information technology and investments. Based on the insights gleaned from references [12-17], the following conclusions can be drawn:

1- Developing high-speed fiber-optic internet infrastructure,
2- Achieving the top rank for the fastest mobile internet speeds in the world with a speed of 238.28 megabits per second and the fourth rank in the list of fastest fixed internet speeds in the world with a speed of 205.77 megabits per second, according to the Speedtest Global Index report in July 2023,
3- Emphasizing and investing high costs in various aspects of the IoE,
4- Widespread use of all-purpose applications like "Dubai Now",
5- Launching and developing specialized applications such as "Dubai Taxi" for airport transfers and "Cafu" for mobile fuel delivery services,
6- Establishing the Dubai Internet City,
7- Creating a media city in Dubai with the aim of enhancing the media position of the United Arab Emirates,
8- Encouraging and attracting large, small, and medium-sized companies worldwide to engage in various IoT sectors, including software development, business services, e-commerce, consulting, sales, and marketing,
9- Launching a smart city project by implementing smart solutions in 17 areas, including smart parking, public transportation, smart street lighting, disaster response, smart payments, connected education, smart tolls, water management, waste management, chronic disease monitoring, employee productivity, smart buildings, surveillance, smart grid, preventive care, drug authenticity, and compliance,
10- Establishing a collection of smart buildings with features such as 24-hour support services, affordable internet connectivity for offices and homes, abundant local and wide area networks, international standard-based multimedia networks, integrated internet telephony with identification systems, digital services network, and wireless communication capabilities, providing regional information services, and a secure network television system,
11- Installing and setting up public free Wi-Fi stations,
12- Beautifying the city using smart palm trees,
13- Creating public access to various mobile applications and websites through embedded stations throughout the city,
14- Providing security and managing emergency situations through city stations, each equipped with a 360-degree infrared CCTV camera and an emergency conditions notification button,
15- Involving young people in projects and programs.

Figure 6 provides an overview of Dubai's strategies in the realm of the Internet of Everything (IoE).



Fig. 6. Overview of Dubai's strategies in the realm of the Internet of Everything (IoE).

3-2- Turkey

While the Internet of Everything technology is not yet widely prevalent in Turkey, the foundations, technologies, and key concepts in this domain have made significant progress within the country. This technology, with its unique capabilities, has brought about significant advancements in various fields in Turkey, ranging from advancements in smart agriculture and livestock breeding to urban traffic management, smart airports, and asset surveillance. Financial results also indicate that this technology has led to increased revenues and reduced operational costs. Leveraging successful experiences and the remarkable benefits of IoT technology, Turkey is on a path towards achieving the vision of the Internet of Everything and enhancing productivity across various sectors of its economy. It is expected that this progress and growth will continue in the future. In other words, based on the findings from the referenced sources [18-21], the following conclusions can be drawn:

1- Achieving a 98.4% mobile phone penetration rate,
2- Advancements in smart agriculture and livestock breeding,

3- Entering cooperation agreements with global giants such as YurtTek, Vodafone, and Binance to facilitate the sales of electronic, cloud, and digital currency products,
4- Collaborating with international telecommunications leaders, including Ericsson, to bolster communication infrastructure,
5- Implementing beacon devices to revolutionize the banking industry and enhance its operations,
6- Utilizing intelligent traffic management systems with high adaptability and adaptive traffic control systems,
7- Establishing an emergency traffic management center and road infrastructure,
8- Enabling diversified vehicle-to-vehicle and vehicle-to-infrastructure communications, including connected and interactive vehicles,
9- Smart parking systems with contactless payment options for drivers,
10- Multi-purpose electronic payment cards,
11- Smart bus stations equipped with information systems tailored for individuals with disabilities using specialized cards,
12- Integration of Internet of Things technology on elevators to enhance performance,
13- Inauguration of an advanced-technology smart airport,
14- Creation of a green urban zone in Istanbul,
15- Implementation of an intelligent traffic signal control system and electronic information dissemination for traffic improvement and communication.

Figure 7 provides an overview of Turkey's strategies in the realm of the Internet of Everything (IoE).



Fig. 7 Overview of Turkey's strategies in the realm of the Internet of Everything (IoE).

3-3- China

In China, rapid and remarkable progress in the development of the Internet of Everything has been observed, and the country's leaders have recognized this tool as a new driver and engine for economic growth and industry. Presently, China stands out as a global leader in the field of the IoE. An accurate and appropriate definition of programs and strategies has played a crucial role in accelerating the advancement of IoE technology in the country [22]. This precise definition has led to an acceleration of progress in the IoE technology sector to the extent that we are witnessing a dazzling demonstration and a sustainable increase in the country's economic revenues. Even in critical situations such as the COVID-19 crisis, this growth has remained steadfast. After reviewing the sources [22-30], the following conclusions are drawn from this study:

1- The National 863 Program,
2- Establishing the framework of Project 973 for national fundamental and key research and development projects,
3- Defining the IoE as a new engine for economic and industrial growth,
4- Utilizing components and equipment of the IoE locally,
5- Building the world's largest FiOS mobile phone network,
6- Achieving the fourth position in mobile network speed globally by shifting policy from "coverage and popularity" to "improving speed and quality",
7- Effectively leveraging the conditions of the COVID-19 pandemic as an opportunity for the development and utilization of IoE technologies,
8- Developing a digital payment platform to facilitate online commerce and transactions,
9- Presenting five-year plans aimed at creating coordination and sustainable development in the field of the IoE,
10- Establishing committees and specialized associations to share experiences and exchange information in the field of IoE development, with government support and holding joint sessions between ministries,
11- Extensive training to strengthen human resources in areas related to IoE technology,
12- Focusing on the production and sale of smart electronic devices to achieve the goals of the IoE in society,
13- Promoting open and public architecture in the field of the IoE,
14- Achieving the second position globally in the smart home sector using advanced technologies,
15- Collaborating with the three major operators to develop and execute joint strategies in the field of IoE technology,
16- Developing smart city development plans aimed at leveraging IoE technologies in various areas,
17- Advancements in smart agriculture to improve efficiency and agricultural production using Internet technologies,
18- Smart procurement to enhance the supply and management of materials and goods using the IoE,
19- Smart transportation by utilizing timely and location-based information to reduce traffic and increase efficiency,
20- Smart network to ensure reliable and sustainable connections between various components of the IoE,
21- Smart environmental preservation using Internet technologies to control and reduce pollution and energy consumption,
22- Smart safety for better prevention and management of accidents and undesirable events,

23- Smart medical care using medical and IoE technologies to enhance healthcare services,
24- Defining the structure of the IoE system for optimal utilization of smart coal mines and oil fields' technologies,
25- Initiating and implementing IoE projects based on space technology to advance spatial and geographical technologies,
26- Government policies granting tax exemptions to IoE sector producers to encourage investment,
27- Encouraging public institutions to invest in IoE projects with government support and facilities,
28- Hiring artificial intelligence experts in the field of autonomous transportation and other IoE applications,
29- Introducing the Internet Plus strategy by the government to maintain and strengthen the country's position in global IoE competition,
30- Utilizing narrowband Internet to increase the speed and efficiency of production and delivery processes for industrial units, smartifying production, mass customization of products, and collaborative innovations in smart product development tools.
31- Establishing a national IoE center for knowledge exchange and experience sharing in various Internet technology fields,
32- Government focus on developing the IoE in vital economic and productive sectors such as industrial control, financial services, and healthcare to increase productivity and quality in these sectors,
33- Utilizing IoE programs to address important urban issues such as air pollution and urban resource management through the implementation of smart city projects at a strategic level and allocating necessary financial resources to municipalities and economic development zones,
34- Emphasizing the creation of fast and cost-effective communications for small and medium-sized companies using the IoE and encouraging these companies to equip their business systems on cloud infrastructures to create extensive entrepreneurship and innovation opportunities,
35- Putting a major focus on enhancing cyber security using a national network to reduce security risks associated with IoE devices and industrial systems connected to the Internet,
36- Prioritizing global leadership in accelerating artificial intelligence progress to transform the country into a major artificial intelligence innovation hub by 2030 with the goal of global leadership in this field,
37- Deciding on the rapid integration of information and communication technology with industrial Internet development sectors to enhance coordination and the development of advanced technologies,
38- Providing cloud infrastructure and open computing platforms for the Internet of Things to integrate with local government public service platforms for modernization and transforming traditional businesses into integrated industrial IoE platforms.

Figure 8 provides an overview of China's strategies in the realm of the Internet of Everything (IoE).

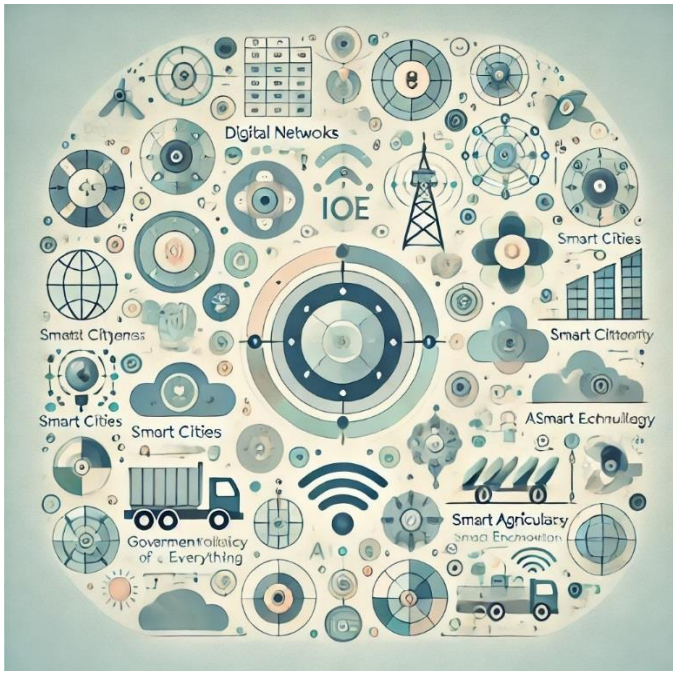


Fig. 8 Overview of China's strategies in the realm of the Internet of Everything (IoE)

3-4- South Korea

South Korea has outlined ambitious visions for the Internet of Everything. As a leader in both economy and the advancement of information and communication technology in the Asian region, South Korea has solidified its position. In 2020, South Korea claimed the top spot in average internet speed when compared to the top 10 high-speed internet countries worldwide. This accomplishment underscores the nation's substantial potential in the field of intelligent transformation and achieving the comprehensive goals of the Internet of Everything. Notably, South Korea's adeptness in establishing smart cities played a crucial role in its success in managing the COVID-19 pandemic. By leveraging secure and dynamic infrastructures, South Korea has managed to develop IoT services and enhance them, resulting in a noteworthy average growth rate of 22.6% within the IoE domain. The results of a survey conducted within South Korea's IoE industry, published by the Ministry of Science and ICT, highlight the most prominent activities among various businesses within the country. These activities primarily include innovations and the export of IoE equipment and services, driving significant growth in the export sector. Following an examination of references [31-38], the following conclusions can be drawn from this study:

1- Developing an open platform through collaboration with platform companies, including large and global businesses, communication service providers, as well as

cooperation in creating a testing infrastructure and standardization,

2- Enhancing public management by addressing existing issues in society, including civil services, improving industry efficiency, effectiveness, and value addition, as well as enhancing aspects related to individuals such as safety, comfort, and quality of life,

3- Establishing a laboratory for innovative equipment to conduct research in specific equipment ecosystems and support creative ideas in the stages of development, production, commercialization, and entry into the global market,

4- Establishing a user-participatory organization called the "Cloud-Connect Society" discussing and exchanging views on various social issues such as regulatory settings, privacy, and the development of quality of life indicators for users,

5- Expanding the platform and services to all industries and countries through pilot services provided by each ministry, local government, or user businesses. This expansion is also carried out through innovation and creative economy centers,

6- Enhancing security technologies in the Internet of Things, including embedded security systems in IoE products and the development and enhancement of information security measures,

7- Expanding access to open laboratories (managed by IoT innovation centers and creative economy centers) and developing and offering new products and services through pilot projects in which users can actively participate and gain hands-on experience,

8- Developing wired and wireless infrastructures to support the Internet of Things and enhancing communication and data transfer capabilities,

9- Strengthening collaboration between the private sector and the government,

10- Establishing research and development programs in the medium and long term for the IoE,

11- Fostering a competitive and open industrial environment for developers and businesses,

12- Opening the platform for small and medium-sized enterprises and universities to develop their own services and products,

13- Utilizing IoE technologies in high-potential production products by small and medium-sized enterprises through localization projects and upgrading products to smarter and better levels,

14- Improving support for the commercialization process in the IoE domain,

15- Enhancing information security infrastructure,

16- Enhancing interaction between software, equipment, or user-related businesses and large, small, and medium-sized companies,

17- Training and developing a skilled and competent workforce in the field of the Internet of Things,

18- Increasing the development and expansion of services tailored to the global market,

19- Creating a platform for testing security capabilities and specifications at an IoE innovation center,

20- Facilitating the secure deployment of additional frequencies of one gigahertz or more,

21- Providing smartphones with free internet to foreign tourists and aggregating and analyzing the data transmitted by these phones,

22- Establishing research and development programs in medium and long terms to turn ideas into products and businesses,

23- Creating an ecosystem to transform ideas into products and services, including open-source hardware or software and full implementation of the process by developers themselves,

24- Developing IoE-based services based on demand from the government, private sector, and citizens in areas such as health, smart homes, smart cities, transportation and logistics, energy, and safety,

25- Enhancing innovative services that combine public and private sector information with data collected from IoT devices in a synchronized manner,

26- Developing creative services with a focus on user experience,

27- Encouraging internal strategy development for large, small, and medium-sized businesses and startups,

28- Developing critical infrastructures such as fiber networks and implementing IPv6 protocol to facilitate and enhance the efficiency of the IoE,

29- Advancing privacy-preserving technologies in the field of IoT,

30- Developing key technologies for the development and commercialization of smart sensors and establishing a connection between research and development in the smart sensor field with demonstration and pilot projects,

31- Strengthening key technologies and creating suitable infrastructure for the development of skilled human resources,

32- Developing products and services through government collaboration with international businesses,

33- Creating and developing an open platform and testing framework to reduce market entry costs and time, and facilitate collaboration between companies,

34- Preparing a comprehensive roadmap for information security in the IoT field and establishing a framework for international cooperation for managing rapid responses and information exchange based on effective sharing,

35- Promoting support for coexistence of traditional industries and new software innovations,

36- Establishing integrated support for all stages of product lifecycle, as well as building and developing model smart cities like Songdo,

37- Developing data hubs for optimal health control in smart city-related projects,

38- Promoting the process of processing and issuing temporary licenses for new products and services,

39- Promoting the development of low-consumption, long-range coverage, and unrestricted bandwidth

communication technologies for connecting objects in remote areas,

40- Promoting the development of new generation technologies for smart devices and components, including wearable devices, health equipment, and very small devices with low energy consumption,

41- Promoting the creation of a smart device industry and developing innovative approaches,

42- Promoting open innovations in the field of IoT,

43- Encouraging collaboration and sharing of research and development between the private sector and military forces to advance military capabilities and excellence in international standards,

44- Strengthening unity and collaboration to ensure the competitiveness of platforms and forming open partnerships based on mutual growth, including collaboration between large, small, and medium-sized companies,

45- Empowering entry into the equipment market with lower costs through the development of open hardware and launching joint growth by companies' collaboration in the production of equipment and components in the process of IoT service development.

Figure 9 provides an overview of South Korea's strategies in the realm of the Internet of Everything (IoE).

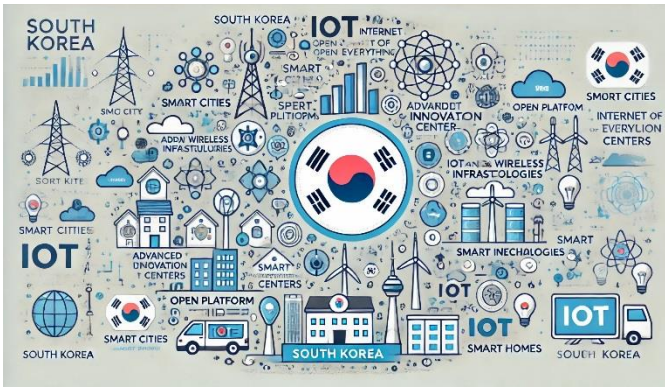


Fig. 9 Overview of South Korea's strategies in the realm of the Internet of Everything (IoE)

3-5- India

With its immensely high potential in the realm of information technology and communications, India has set forth on a trajectory of developing and adopting Internet of Everything technology. Based on predictions, in the not-so-distant future, this country will become the most populous nation in the world. Through an exploration of the programs, projects, and strategies implemented in this field, it is evident that India is reaping the benefits of IoT technology across various economic, social, and security domains. Collaborations with international partners and effective policies play a pivotal role in its successful adoption. Emphasizing the establishment of knowledge hubs in other countries and attracting investments in service provision, India strives to advance higher education and facilitate knowledge exchange with other nations. The advancement of information technology, enhancement of higher education systems, globalization, and alignment with the global job market serve as key determinants of India's developmental trajectory. India's experience underscores that, with a suitable approach, IoE technology can guide societal and economic transformations towards sustainable development. Upon reviewing references [39-49], the following conclusions can be inferred:

1- Clarifying the concept of Digital India through the establishment of a network of 100 smart cities,

2- Creating a government data portal for transparency and access to information,

3- Progressing towards smart parking using modern technology,

4- Designing and implementing an intelligent transportation system to enhance coherence and efficiency,

5- Establishing smart networks to enhance communication and information sharing,

6- Optimizing urban lighting in an intelligent manner for energy efficiency,

7- Enhancing intelligent waste management through the utilization of new technologies,

8- Improving intelligent water resource management with a modern and efficient approach,

9- Focusing on harnessing the potential of the market for smart electronic devices to increase sales,

10- Utilizing IoT technology to enhance border services and transportation centers,

11- Establishing university campuses in other countries and attracting investments in providing scientific services,

12- Utilizing the potential of the Internet of Things technology to ensure the security of critical sectors, including industries, banks, offices, nuclear power plants, and other facilities,

13- Implementing intelligent image management systems for recording and detecting unusual events, identifying individuals, locations, and recognizing colors using precise and informational methods,

14- With advancements in the field of tracking applications for patients, important information, including job details, geographic coordinates, contact information, ecological aspects, travel history, and biological data such as fingerprint information, can be gathered, considering the new conditions created by the emergence of the coronavirus,

15- Develop an Internet of Things roadmap with five vertical columns, including centers for testing and executing projects, growth and incubation centers, innovation and research and development areas, support and motivation, as well as human resources and support development; and a horizontal column encompassing standards and governmental structure,

16- Proposing an intelligent tsunami alert service,

17- Designing and implementing an Internet of Things-based communication system,
18- Establishing a smart system for electronic payment of fees,
19- Experiencing remarkable growth in the information and communication technology sector, with a 1000-fold increase since 1993,
20- Increasing the volume of exports of information technology and communication services with a special emphasis on expanding this economic sector,
21- Allocating 80% of machine-to-machine (M2M) communications to the South Asia region,
22- Youth make up the majority of active users of smart systems,
23- Active participation and collaboration with international partners and leveraging the experiences of global associations, as well as cooperating and consulting with leading countries in the field of IoE,
24- Establishing open platforms with the aim of facilitating usage and reducing costs, and designing scalable models as key factors for success in the IoE domain,
25- Employing citizens as live sensors to maximize benefits and transparently collect data.

Figure 10 provides an overview of India's strategies in the realm of the Internet of Everything (IoE).



Fig. 10 Overview of India's strategies in the realm of the Internet of Everything (IoE)

3-6- Malaysia

The roadmap for the Internet of Things in Malaysia stands out among the wealth of documents available for examining various the Internet of Everything initiatives. This roadmap serves as a comprehensive guide, covering the readiness, opportunities, and challenges of IoT communications in Malaysia. This document presents an analysis of Malaysia's current and future position in the IoT domain, encompassing infrastructure, data and information, security, ecosystem, and potential. It then delves into dissecting the gaps. Based on conducted studies, Malaysia's readiness to embrace IoT communication technology, including mobile penetration and internet accessibility, demonstrates a conducive ground for IoT development. This platform facilitates economic innovation opportunities and enables the technology to serve as a platform for commercializing research outcomes by research organizations. Moreover, the importance of striking a balance between development and security in this domain is emphasized in this roadmap. It suggests that with advancements in this field, Malaysia could be recognized as a central hub and regional focal point for IoT development [50]. The country's young generation has shown significant interest in the internet, not just as consumers but also as creative developers. Through studying references [51-57], the following conclusions can be drawn:

1- Formulating a comprehensive roadmap for IoT development,
2- Defining and elucidating key performance indicators in the field of IoE,
3- Empowering and elevating small and medium enterprises as capacity-building factors in the IoE sector,
4- Enhancing collaboration and cooperation between research and development sectors, in both private and governmental domains,
5- Establishing an integrated center for the development and provision of various products, services, and solutions in the IoE domain,
6- Crafting and presenting strategic budgets for advancing crucial initiatives in this domain,
7- Gathering real-time data, integrating resources, and sharing them to achieve optimal utilization and efficient system integration and monitoring,
8- Providing a comprehensive and central approach for urban advancement to foster sustainable and extensive growth,
9- Encouraging continuous diagnosis and precise medical treatment by medical professionals using IoE technologies, including wearable devices that record and analyze vital signs and dietary habits.
10- Establishing a dedicated organizational structure in the IoE domain,
11- Establishing digital economic connections with China within the framework of the Belt and Road Initiative,
12- Creating an open innovation framework and proposing innovative solutions,

13- Strengthening prominent cities in the field of information technology, such as Cyberjaya,

14- Implementing IoT pilot projects in various sectors including agriculture, aquaculture, healthcare, government, and environment,

15- Generating motivation and opportunities for active participation from local industries and collaborating with multinational corporations to enhance the development, dissemination, and adoption of IoT technologies,

16- Forming cyber consortia and alliances in the IoT sector and attracting leading companies such as Kaspersky for collaboration,

17- Establishing specialized laboratories for the creation and development of practical projects,

18- Enhancing and nurturing specialized talents in the IoE domain and expanding knowledge and technology-related skills in this field.

19- Establishing a regulatory and central authority institution for issuing certifications and overseeing the preservation of privacy, security, quality, and relevant standards in the IoE domain,

20- Developing a working framework for mutual communication that can leverage capabilities for rapid development and implementation of IoE in the face of heterogeneity and complexity of various standards and technologies,

21- Providing necessary infrastructure to facilitate easy access to public data,

22- Creating a collaboration framework to connect small and medium-sized enterprises with leading multinational corporations and leveraging their experiences and resources.

Figure 11 provides an overview of Malaysia's strategies in the realm of the Internet of Everything (IoE).



Fig. 11 Overview of Malaysia's strategies in the realm of the Internet of Everything (IoE)

4- Results and Discussion

The empirical analysis of the experiences of the countries discussed in this article can serve as a model and inspiration for other nations in achieving the Internet of Everything and device-to-device interactions. As we have seen, Dubai, one of the seven emirates of the United Arab Emirates, has taken significant strides towards implementing the Internet of Everything. By deploying smart infrastructure, launching the unified Dubai Now app for all government and city services, and establishing a smart city, Dubai has achieved the distinction of having the fastest mobile internet speed in the world and the fourth fastest in fixed internet in 2023 among its neighboring countries. Therefore, it stands as an excellent example of innovation in pursuing the visions of the Internet of Everything for neighboring nations.

In contrast, in another neighboring country, Turkey, Internet of Everything technology had not yet reached the implementation stage, but the foundational elements, technologies, and key concepts of the Internet of Everything have been well established. Turkey has made notable progress in building the Internet of Everything infrastructure. This progress includes the development of a low-bandwidth Internet of Things ecosystem and a favorable environment for 5G technology. Additionally, Turkey has executed numerous smart projects in areas such as urban development, transportation, public welfare, agriculture, livestock, telecommunications, and banking. We can observe that Istanbul, in comparison to two other

green cities, Copenhagen and Kiev, has a compelling story to tell in terms of its green initiatives.

China, a developed nation with a robust human development index, the progress and development of the Internet of Everything has gained, with its leaders defining it as a new engine for economic growth and industry. Viewing transformation as an opportunity rather than a threat, the new circumstances brought about by the COVID-19 pandemic have not only failed to slow down China's advancement in Internet technology but have also contributed to a continuous increase in the country's income. The designation of national programs like the 863 Program, the 973 Research Framework, and the development of fundamental and key national projects under the guidance of the Chinese Ministry of Science and Technology, along with the collaboration of the three major Chinese operators (e.g., telecommunications companies), has been pivotal in the development of the Internet of Everything in China.

South Korea, another developed nation, which ranks among the top Asian countries in terms of economic and information technology development, boasts the highest average internet speed among the world's top 10 fastest countries, showcasing its immense potential in various smartization domains and realizing the Internet of Everything vision. This accomplishment has played a role in South Korea's success in controlling the COVID-19 pandemic, as evidenced by its smart city initiatives. South Korea has harnessed secure and dynamic infrastructure for the development of Internet of Everything services, underpinned by a comprehensive strategic plan and necessary actions. The country achieved an impressive 22.6% growth in the Internet of Everything sector from 2015 to 2018. The results of surveys conducted on the Internet of Everything industry in South Korea from 2015 to 2019, overseen by the Ministry of Science and ICT, indicate that in 2019, the highest exports were in terms of business in the equipment sector, and the highest exports in terms of application were in the manufacturing and retail sectors.

India, a developing nation, envisions becoming the world's most populous country in the near future. The Digital India program aims to transform India into a powerful digital society and knowledge-based economy. This initiative has inspired India to allocate a substantial budget of around $7.4 billion for expanding the Internet of Everything, fostering partnerships with leading universities globally, and planning the development of smart cities. Some of the key components of the smart city agenda that have received attention in India include the government open data portal, smart parking systems, intelligent transportation systems, healthcare and patient tracking, smart grids, smart street lighting, waste management, digital signage, border security, and water management. Consequently, India witnessed an increase in sales revenue for smart electronic devices from 2019 to 2020, while other top countries in this sector experienced a declining trend due to the conditions arising from the COVID-19 pandemic. Overall, India's information technology sector has seen consistent annual growth of over 30% since 1993, and its market value has grown from $150 million to $150 billion, marking a thousand-fold increase. The technology industry in India indeed holds immense potential for growth and development. India's proposed roadmap for the IoT is a multi-pronged approach, consisting of five vertical columns: Testing and project implementation centers, growth centers and incubators, innovation and research and development, support and motivation, and human resource development and support, with two horizontal columns of standards and governmental structure.

Lastly, Malaysia, another developing country, has created a roadmap for IoE readiness. Among the rich documents in studying comprehensive plans in countries, the roadmap for the IoT in Malaysia plays a significant role. In this roadmap, Malaysia's current status in terms of readiness and opportunities for the Internet of Things, as well as the challenges ahead in areas such as infrastructure, data and information, security, and privacy, talent, and the ecosystem have been assessed. Gap analysis was conducted subsequently. Indicators of information and communication technology (ICT) readiness, such as mobile and internet penetration rates and other metrics in Malaysia, indicate a conducive environment for the development of IoT services, given domestic demand. This readiness has created unique opportunities to unlock Malaysia's economic innovation potential, particularly in transformational programs across the economy, government, and digital lifestyles. However, this opportunity is highly valuable for research institutions aiming to commercialize research and development results, which require an appropriate platform for implementing solutions.

In summation, exploration of these diverse countries' IoE journeys provides valuable insights into IoE's multifaceted implementation and its potential impact on various sectors. These case studies serve as reference points for other nations looking to navigate the evolving landscape of the Internet of Everything and capitalize on its myriad benefits.

5- Conclusion

In conclusion, this article offers a comprehensive summary of key achievements and strategies in the pursuit of the Internet of Everything in select nations. The diverse case studies furnish valuable insights and impetus for government officials, researchers, managers, and entrepreneurs venturing into the realms of digital transformation and emerging technologies. The transition toward the IoE has created abundant opportunities and challenges for various countries. In the case studies of China, South Korea, Malaysia, India, Turkey, and the United Arab Emirates, it has been observed that each

country, based on its characteristics, resources, and objectives, has pursued unique strategies and approaches to achieve the goals of the Internet of Every Thing. These experiences can serve as models and sources of inspiration for other countries in their endeavors to realize the IoE and harness the interactions among devices and objects. For instance, Dubai has rapidly become a global leader in mobile internet and fixed internet speed, showcasing innovative IoE implementation. In contrast, Turkey has established a robust foundation for IoE, focusing on low-bandwidth IoT ecosystems and implementing smart initiatives across various sectors. China's dedication to the IoE, as seen in its national programs, has driven economic and industrial growth. South Korea's swift internet speeds have laid the groundwork for successful IoE initiatives, especially in smart city development. India, with its Digital India program, is actively investing in IoE expansion, aiming to develop 100 smart cities. Malaysia, too, has outlined a strategic IoE roadmap, emphasizing infrastructure, data, security, privacy, talent, and ecosystems. These case studies offer valuable insights for policymakers, researchers, managers, and entrepreneurs venturing into digital transformation and emerging technologies.

References

[1] A. Khamseh, M.A. Mirfallah Lialestani, R. Radfar, "Digital Transformation Model, Based on Grounded Theory", Journal of Information Systems and Telecommunication (JIST), Vol. 9, No. 36, 2021, pp. 275-284.

[2] M. Khazaei, "Dynamic Tree-Based Routing: Applied in Wireless Sensor Network and IoT", Journal of Information Systems and Telecommunication (JIST), Vol. 10, No. 39, 2022, pp. 191-200.

[3] M. Ranjbarfard, S.R. Mirsalari, "IT Capability Evaluation through the IT Capability Map", Journal of Information Systems and Telecommunication (JIST), Vol. 8, No. 32, 2021, pp. 207-218.

[4] K. Bamary, M.R. Behboudi, T. Abbasnjad, "An ICT Performance Evaluation Model based on Meta-Synthesis Approach", Journal of Information Systems and Telecommunication (JIST), Vol. 10, No. 39, 2022, pp. 229-240.

[5] FREEDOM and SAFETY, "This is The Internet of Everything", https://freedomandsafety.com/en/file/ioepng, Site Visited: 2024.

[6] James Macaulay, Lauren Buckalew, Gina Chung, "Internet of Everything in Logistics", a collaborative report by DHL and Cisco on implications and use cases for the logistics industry, 2015.

[7] P.N. Huu, L.H. Bao, "Proposing Real-time Parking System for Smart Cities using Two Cameras", Journal of Information Systems and Telecommunication (JIST), Vol. 9, No. 36, 2021, pp. 252-262.

[8] N.P. Singh, A. Kanakamalla, S.A. Shahzad, G.D. Asi, S. Suman, "Remote Monitoring System of Heart Conditions for Elderly Persons with ECG Machine using IoT Platform", Journal of Information Systems and Telecommunication (JIST), Vol. 10, No. 37, 2022, pp. 11-19.

[9] M. Little, S. Kechiche, Y. Zhong, A. Gharibian, "Realising the Potential of IoT in MENA", GSMA Intelligence report, 2019.

[10] Radwa Ahmed Osman, "Empowering Internet-of-Everything (IoE) Networks through Synergizing Lagrange Optimization and Deep Learning for Enhanced Performance", ElSEVIER, Physical Communication, Vol. 63, 2024, Article ID 102309 .

[11] D. J. Langleya, J. Van Doorn, I. C.L. Ng, S. Stieglitz, A. Lazovik, A. Boonstra, "The Internet of Everything: Smart Things and Their Impact on Business Models", ElSEVIER, Journal of Business Research, Vol. 122, 2021, pp. 853-863.

[12] Y. Koucheryavy, A. Aziz, "Internet of Things, Smart Spaces, and Next Generation Networks and Systems", Springer Link, 23rd International Conference, NEW2AN, and 16th Conference, ruSMART, 2023, Part II Dubai, United Arab Emirates, Proceedings.

[13] OpenSignal, "Benchmarking the Global 5G Experience", 2021.

[14] Cisco, "Dubai Harnesses IoE to Make Roads Safer and to Increase Usage of Public Transportation", Cisco Jurisdiction Profile, 2014.

[15] C. Reberger, F. Atallah, M. Zeidan, S. Ei, "AED 17.9 bn Opportunity for Dubai: 2014-2019", 2020.

[16] S. Eid, "Dubai Smart City: IoE Value at Stake in the Public Sector", Cisco Consulting Services Lead for Middle East Africa Russia CIS, 2020.

[17] Speedtest, "United Arab Emirates Median Country Speeds July 2023", https://www.speedtest.net/global-index/united-arab-emirates, 2023.

[18] M. Little, S. Kechiche, Y. Zhong, A. Gharibian, "Realising the potential of IoT in MENA", GSMA InteIlligence report, 2019.

[19] OPENSIGNAL, "TURKEY Mobile Network Experience Report", https://www.opensignal.com/reports/2020/12/turkey/mobile-network-experience, 2021.

[20] H.H. Çelikyay, "The Studies through Smart Cities Model: The Case of Istanbul", International Journal of Research in Business and Social Science, Vol.6, No.1, 2017, pp.149-163.

[21] G. Bodur, S. Gumus, N. Gul Gursoy, "Perceptions of Turkish Health Professional Students Toward the Effects of the Internet of Things (IOT) Technology in the Future", ElSEVIER, Nurse Education Today, Vol. 79, 2019, pp. 98-104.

[22] W. Wu, L. Shen, Z. Zhao, A. Rachana Harish, R.Y. Zhong, G.Q. Huang, "Internet of Everything and Digital Twin Enabled Service Platform for Cold Chain Logistics", ElSEVIER, Journal of Industrial Information Integration, Vol. 33, 2023, Article ID 100443.

[23] A. Bouverot, "How China is Scaling the Internet of Things", An insight report from the GSMA Connected Living Programme, 2015.

[24] J. Chen, and et al, "China's Internet of Things", Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission, 2018.

[25] Jing Dai, Wen Che, Jia Jia Lim, Yongyi Shou, "Service Innovation of Cold Chain Logistics Service Providers: A Multiple-Case Study in China", ElSEVIER, Industrial Marketing Management, Vol. 89, 2020, pp. 143-156.

[26] S. Chen, H. Xu, D. Liu, Hu, H. Wang, "A Vision of IoT: Applications, Challenges, and Opportunities with China Perspective", IEEE Internet of Things Journal, Vol. 1, No. 4, 2014, pp. 349-359.

[27] Statista, "COVID-19 Barometer 2020", https://www.statista.com/study/72001/covid-19-barometer, 2020.

[28] Ant Group, KrASIA, https://kr-asia.com/ant-group-searches-for-direction-in-a-new-era-of-chinese-fintec, Site Visited: 2024.

[29] M. Granryd, "How Greater China is Set to Lead the Global industrial IoT", A GSMA Internet of Things report, 2018.

[30] M. Farhan, T.N. Reza, F.R. Badal, M.R. Islam, S.M. Muyeen, Z. Tasneem, M.M. Hasan, M.F. Ali, M.H. Ahamed, S.H. Abhi, M.M. Islam, S.K. Sarker, S.K. Das, P. Das, "Towards Next Generation Internet of Energy System: Framework and trends", ElSEVIER, Energy and AI, Vol. 14, 2023, Article ID 100306.

[31] M. Waszkiewicz, "Internet of Things South Korea", Market Intelligence Report, Department for International Trade Report, prepared by Intralink Limited, 2018.

[32] M. Lee, "An Empirical Study of Home IoT Services in South Korea: The Moderating Effect of the Usage Experience", International Journal of Human-Computer Interaction, Vol. 35, Issue. 3, 2018, pp. 1-13.

[33] R. Triggs, "Which Country Has the Fastest Mobile Network?", https://www.androidauthority.com/worlds-fastest-networks-709140/, 2017.

[34] S. Muralidharan, A. Roy, N. Saxena, "An Exhaustive Review on Internet of Things from Korea's Perspective", Springer Link, Wireless Personal Communications, Vol. 90, 2016, pp. 1463-1486.

[35] IoT Business News, "The Countries with the Most IoT Devices, Ranked", https://iotbusinessnews.com/2016/03/31/97541-countries-iot-devices-ranked, 2016.

[36] Ministry of Science, ICT and Future Planning, "Master Plan for Building the Internet of Things (IoT), That Leads the Hyper-Connected, Digital Revolution", Software Policy Bureau, New Internet Industry Division, 2014.

[37] Internet World Stats, "Internet 2021 Usage in Asia, the World's Fifth Largest Market", Usage and Population Statistics, https://www.internetworldstats.com, 2021.

[38] Business Korea, Korea's Premium Business News Portal, "S. Korea's IoT Sales Reach 8.6 Tril. Won in 2018", http://www.businesskorea.co.kr, 2019.

[39] Statista, "Total Number of Internet of Things (IoT) Patent Applications Worldwide as of 2019, by Country", https://www.statista.com/statistics/992140/worldwide-internet-of-things-patent-applications-country, 2019.

[40] Statista Global Consumer Survey, https://www.statista.com/global-consumer-survey, site visited: 2024.

[41] S. Chatterjee, A.K. Kar, "Regulation and Governance of the Internet of Things in India", Digital Policy, Regulation and Governance, 2018, Vol. 20 No. 5, pp. 399-412.

[42] Statista Consumer Market Outlook, https://www.statista.com/outlook/consumer-markets, Site Visited: 2024.

[43] S. Chatterjee, A.K. Kar, Y. K. Dwivedi, "Intention to Use IoT by Aged Indian Consumers", Journal of Computer Information Systems, 2022, Vol. 62, No. 4, pp. 655-666.

[44] Statista Global Consumer Survey, https://www.statista.com/global-consumer-survey, Site Visited: 2024.

[45] S., A.K. Kar, M.P. Gupta, "Success of IoT in Smart Cities of India: An empirical Analysis", ElSEVIER, Government Information Quarterly, 2018, Vol. 35, Issue. 3, pp. 349-361.

[46] India Open Government Data (OGD), https://data.gov.in, Site Visited: 2024.

[47] Ministry of Electronics & Information Technology, Government of India, "IoT Policy Document", Department of Electronics & Information Technology (DeitY), https://www.meity.gov.in, 2016.

[48] S. Chatterjee, A.K. Kar, S.Z. Mustafa, "Securing IoT Devices in Smart Cities of India: from Ethical and Enterprise Information System Management Perspective", Enterprise Information Systems, Vol. 15, No. 4, 2021, pp. 585-615.

[49] Statista Technology Market Outlook, https://de.statista.com/outlook/technology-outlook, Site Visited: 2024.

[50] S.O. Azarkasb, S.H. Khasteh, "Strategies and Ecosystem Transformations in the Internet of Everything in Malaysia", Journal of Industry & University, ISC, Vol. 55-56, 2024, pp. 187-204.

[51] RICOH, "5 Pillars of Malaysia Cyber Security Strategy 2020-2024", https://www.ricoh.com.my, 2023.

[52] TELECOM Review, "Malaysia's Digital Transformation Powered by New Technologies", https://www.telecomreviewasia.com/news/featured-articles/4001-malaysia-s-digital-transformation-powered-by-new-technologies/, 2024.

[53] B-K Chery, B-K Ng, C-Y Wong, "Governing the Progress of Internet-of-Things: Ambivalence in the Quest of Technology Exploitation and User Rights Protection", ELSEVIER, Technology in Society, Vol. 64, 2021, Article ID 101463.

[54] Y.Yuan, T. C. Cheah, "A Study of Internet of Things Enable Hesalthcare Acceptance in Malaysia", Journal of critical reviews, Journal of Critical Reviewe, Vol. 7, No. 3, 2020.

[55] A.H. Abdul Halim, and et all, "National Internet of Things (IoT) Strategic Roadmap", MIMOS BERHAD, Technology Park Malaysia, 2015.

[56] M. A. Musarat, W.S. Alalou, A.M. Khan, S. Ayub, b, Na. Jousseaume, "A Survey-Based Approach of Framework Development for Improving the Application of Internet of Things in the Construction Industry of Malaysia", ELSEVIER, Results in Engineering, Vol. 21, 2024, Article ID 101823.

[57] MIMOS BERHAD, Technology Park Malaysia, "National Internet of Things (IoT) Strategic Roadmap: A Summary", 2015.

Journal of Information Systems and Telecommunication
Vol.12, No.3, July-September 2024, 233-241
http://jist.acecr.org
ISSN 2322-1437 / EISSN:2345-2773

GOA-ISR: A Grasshopper Optimization Algorithm for Improved Image Super-Resolution

Bahar Ghaderi[1], Hamid Azad[1]*, Hamed Agahi[1]

[1].Department of Electrical Engineering, Shi. C., Islamic Azad University, Shiraz, Iran

Received: 03 Dec 2023/ Revised: 04 Sep 2024/ Accepted: 14 Oct 2024

Abstract

The image super-resolution (ISR) process provides a high-resolution (HR) image from an input low-resolution (LR) image. This process is an important and challenging issue in computer vision and image processing. Various methods are used for ISR, that learning-based methods are one of the most widely used methods in this field. In this approach, a set of training images is used in various learning based ISR methods to reconstruct the input LR image. To this end, appropriate reconstruction weights for the image must be computed. In general, the least-squares estimation (LSE) approach is used for obtaining optimal reconstruction weights. The accuracy of SR depends on the effectiveness of minimizing the LSE problem. Therefore, it is still a challenge to obtain more accurate reconstruction weights for better SR processing. In this study, a Grasshopper Optimization Algorithm (GOA)-based ISR method (GOA-ISR) is proposed in order to minimize the LSE problem more effectively. A new formulation for the upper bound and the lower bound is introduced to make the search process of the GOA algorithm suitable for ISR. The simulation results on DIVerse 2K (DIV2K) dataset, URBAN100, BSD100, Set 14 and Set 5 datasets affirm the advantage of the proposed GOA-ISR approach in comparison with some other basic Neighbor Embedding (NE), Sparse Coding (SC), Adaptive Sparse, Iterative Kernel Correction (IKC), Second-order Attention Network (SAN), Sparse Neighbor Embedding and Grey Wolf Optimizer (GWO) methods in terms of Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM). The results of the experiments show the superiority of the proposed method comparing to the best compared method (DWSR) increases 8.613 % PSNR.

Keywords: Super Resolution (SR); High-Resolution (HR); Low-Resolution (LR); Learning-based Methods; Grasshopper Optimization Algorithm (GOA).

1- Introduction

The super-resolution (SR) process creates a high-resolution (HR) image using low-resolution (LR) images[1]. In other words, it converts LR images to HR images [2]. This process has been used in HDTV [3], image manipulation [4], face recognition [5], medical imaging [6], remote sensing [7], and monitoring [8]. In general, image SR methods can be divided into three categories: interpolation-based methods [9, 10], reconstruction-based methods [11, 12], and learning-based methods [13, 14]. In interpolation-based methods and reconstruction-based methods, only the features of the input LR images are used to produce a HR image. In learning-based methods, however, the information of external images along with input LR image is used to produce HR image [15]. Learning-based methods have received more attention in recent years due to their superiority for the SR process. [15-18]

Learning-based SR methods can be classified into two categories: global image-based approaches and local patch-based approaches [19]. In global image-based approaches, the entire content of the input LR image is used, whereas in the local patch-based approaches, the content of the input LR image is divided into several parts, and each part is used separately to recover the HR image. Local patch-based methods are more suitable than global based-methods for image reconstruction. [20, 21]

In [22], a local learning-based method was presented for the SR image processing task. In this method, a local training set was developed according to the similarity between the training samples and the test sample, and the local regression function was used on the local training set.

In [23], local and non-local learning-based methods of LR images were proposed for the SR process. In this method, the non-local mean filter was used for the non-local learning, and the regression of the steering kernel was used for local learning.

In [24], the multi-scale similarity learning method was presented for the SR process. In this approach, the input LR image patch was first iterated several times at the same scale and also across different scales. Then, HR-LR patch pairs were created to preserve details, using the original LR input and its down-sampled version to extract similarities at different scales from the images. The neighbor embedding algorithm was finally used to estimate the relationships between LR and HR image pairs.

In [25], a joint SR model was proposed, which had the advantages of the external and the internal SR methods. Two loss functions, (sparse coding-based external samples and epitomic matching-based internal samples) were used in this method.

In [26], a new local learning method, which was based on the kernel ridge regression (KRR), was presented for the SR process. Gabor filter was used to extract texture information from LR patches as features. Then, each input LR feature patch was used by the K-nearest neighbor algorithm to create a local structure. Finally, the KRR was used to map the input LR feature patches to HR feature patches in the local structure.

In [27], an SR approach was proposed based on extreme learning machine (ELM). In the training phase of algorithm, the high-frequency components of the original HR images were given as target values and the image features of the LR images were imported to the ELM to learn a model. In this method, the details and fine structures in LR images were reconstructed well.

In [28], a new method based on non-negative neighbor embedding was presented for the SR process. In this method, a dictionary containing patches of LR images and patches of HR images was used for training. Each LR feature vector in the input image was expressed as the weighted combination of its K nearest neighbors in the dictionary; the corresponding HR feature vector was reconstructed under the assumption that the local LR embedding was preserved.

In all these learning-based methods, the optimal reconstruction weights are obtained by calculating the least-squares error between the input LR image and training LR patches, and then the generated weights are applied to the same HR training patches to reconstruct the output HR patch. All reconstructed HR patches are finally combined together to create a complete HR image. The accuracy of SR depends on the effectiveness of minimizing the least-squares error problem. Therefore, it is still a challenge to obtain more accurate reconstruction weights for better SR processing. The various meta-heuristic algorithms introduced so far can be used for obtaining the weight value for the optimum reconstruction. The grasshopper optimization algorithm (GOA) [29] is one of these methods. This algorithm was introduced by Saremi [29] based on the cooperative behavior of grasshoppers in 2017. The GOA has been widely used in various applications, such as the digital watermarking [30], cancer classification [31], and medical image fusion [32]. Compared to other meta-heuristic algorithms, including Genetic Algorithm (GA) [33], Particle Swarm Optimization (PSO) [34, 35], Firefly Algorithm (FA) [36, 37], Bat Algorithm (BA) [38], and Gravitational Search Algorithm (GSA) [39, 40], this algorithm can avoid local optima, showing a good balance between exploration and exploitation, due to the high amount of exploitation and convergence features. These advantages encouraged the proposal of the GOA for the optimal reconstruction weight value in the SR process.

The rest of this study are organized as follows. Section II is dedicated to a review of GOA. In Section III and Section IV, the proposed method and the simulation results are presented respectively. Section V represents the conclusions of the study.

2- Grasshopper Optimization Algorithm (GOA)

As chewing herbivorous insects, grasshoppers are one of the largest groups among all those creatures. The unique aspect of a cloud of grasshopper is that the group life behavior can be observed in both adult and infant grasshoppers. Millions of newborn grasshoppers jump and move like spinning cylinders. As they become older, they form a group in the air. This is how grasshoppers migrate over long distances. The main characteristic of these groups in the larval stage is the slow movement and small steps of the grasshoppers. In contrast, prolonged and sudden movement is a key feature of these groups among older grasshoppers. Searching for food resources is an important feature of group life among grasshoppers [41]. The life of these insects and their group search for food were the inspirations for generating the GOA. Nature-inspired algorithms generally split the search process into two phases: the exploration and the exploitation. In the exploration phase, search agents are stimulated to move abruptly while tending to passage locally during the exploitation step. These two operations as well as searching for the target are done instinctively by the grasshoppers. The mathematical model for simulating the group behavior of the grasshopper's movements is described according to Equation (1). [29]

$$X_i = S_i + G_i + A_i \tag{1}$$

Where X_i defines the location of the i^{th} grasshopper, S_i is the so-called interaction computed according to Equation (2), G_i is the gravity force on the i^{th} grasshopper, and A_i represents the wind advection [41]. To provide a random behavior, Equation (1) is rewritten as $X_i = r_1 S_i + r_2 G_i + r_3 A_i$ where r_1, r_2 and r_3 are random numbers belong to $[0,1]$. The interaction is calculated using the following equation. [29]

$$S_i = \sum_{j=1}^{N} s(d_{ij})\hat{d}_{ij}, \quad j \neq i \tag{2}$$

Where d_{ij} is the distance between i^{th} and j^{th} grasshoppers computed as $d_{ij} = |x_j - x_i|$, and $\hat{d}_{ij} = (x_j - x_i)/d_{ij}$ is a unit vector from the former grasshopper to the latter one. Moreover, *s* is a function that defines the strength of social forces according to Equation (3). [29]

$$s(r) = f.\exp(-r/l) - \exp(-r) \tag{3}$$

Where *f* represents the intensity of attraction, and *l* is the attractive length scale. The detailed description of the GOA is available in the main references [41, 42]. In an optimization problem involving p parameters, a vector of length *p* is constructed, representing the position of an individual grasshopper within a swarm consisting of multiple insects. According to Equation (1), the position of each grasshopper in the swarm is updated, with respect to the mentioned factors and the optimization objective function in each iteration. After a specified number of iterations, the grasshopper with the optimal objective function is selected as the best answer for the optimization problem.

3- Proposed Grasshopper Optimization Algorithm-Based Image Super-Resolution Method

In this article, a new approach based on the GOA is proposed to obtain optimal reconstruction weights in the SR process. First, each of the input LR image and LR training images is divided into several patches. Then, the distance between each input LR patch and the same patch position in all the LR training images is calculated according to Equation (4).

$$d_{n,m} = \left\| I_n^L - T_{n,m}^L \right\|_2^2 \quad n = 1,2,...,N \quad m = 1,2,....,M \tag{4}$$

Where I^L and T^L are input LR image and LR training images, respectively, *n* is the number of patches, and *m* is the number of LR training images.

The upper bound and lower bound are then calculated according to equations 5 and 6 to limit the spatial range of searching for optimal weights. The GOA is used as the optimizer for the objective function in Equation (7). This algorithm returns the optimal weight vector $w_{n,m}$ for the input patch I_n^L calculated from the same position training LR patches, i.e., $T_{1,1}^L, T_{1,2}^L, T_{1,3}^L, ..., T_{1,M}^L$. The generated weight vectors for each patch are finally used with similar patches in the training HR images to reconstruct the super-resolved patch according to Equation (8). All the $I_{n,m}^H$ patches are combined to create the final HR image. In overlapping regions, the final value is the average of pixel values. The flowchart and pseudo-code of the proposed method are shown in Fig. 1 and Fig. 2, respectively.

$$UB_{n,m} = \frac{1}{d_{n,m}} \times \lambda_1 \tag{5}$$

$$LB_{n,m} = \left| 1 - \frac{1}{d_{n,m}} \times \lambda_2 \right| \tag{6}$$

$$w_{n,m}^* = \arg_{w_{n,m}} \min \left\| I_n^L - T_{n,m}^L w_{n,m} \right\|_2^2 \tag{7}$$

$$I_{n,m}^H = \sum_{m=1}^{M} \sum_{n=1}^{N} T_{n,m}^H w_{n,m} \tag{8}$$

The λ_1 and λ_2 are adjustable parameters with fixed values.

Algorithm 1: Pseudo-code of the proposed GOA-ISR method in the SR process

Input: LR input image, LR and HR training sets:
Output: Output HR image

- *Each LR input image and LR training images are divided into 4×4 size patches.*
- *Each HR training image is divided into 16×16 size patches.*
- *For* $n=1$ $n = 1,2,...,N$

Select patch I_n^L *form* I^L

Compute similarity between input patch and training patches according to Equation (4), and they are sorted in ascending order in a vector then.

Calculate the upper bound and lower bound according to equations (5 and 6)

Call the GOA with cost function:

Obtain the optimal from the GOA $w_{n,m}$

Create HR patches using training HR patches and optimal weights

- *End for*
- *Combine all the* $I_{n,m}^H$ *patches to make the final HR image*

Fig. 1. Pseudo-code of the proposed GOA-ISR method in the SR process

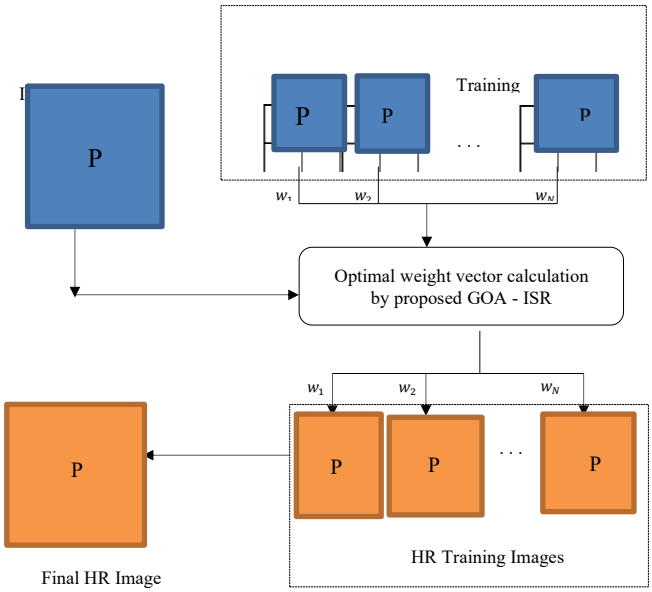


Fig.2. Description of the proposed *GOA-ISR* method First, optimal reconstruction weights are achieved by expressing an input patch in-terms of training LR patches using proposed GOA-ISR. Then, generated weights are applied to counterpart HR training patches for reconstructing the output patch. Finally, all reconstructed patches are joined to build a complete final HR image

4- Implementation and Examination of the Results

In this section, a comprehensive evaluation of the proposed GOA-ISR method is conducted, comparing it against existing methods, including Bicubic [9], Neighbor Embedding (NE) [43], Sparse Coding (SC) [44], Iterative Kernel Correction (IKC) [45], Sparse Neighbor Embedding [46], Adaptive Sparse [47], Second-order Attention Network (SAN) [48], and Grey Wolf Optimizer (GWO) [19]. All of the experiments are performed using MATLAB® 2019A software on a personal computer with an Intel Core i7 processor and 16G RAM. Two databases are used in order to examine the capability of the suggested GOA-ISR method. The database of natural images includes thousands of high-quality and low-quality images [44]. The DIV2K database is published by *Timofte et al.* for ISR [49]. DIV2K consists of 800 training images, 100 validation images, and 100 test images.

4-1- Evaluation Criteria

To evaluate the effectiveness of the proposed GOA-ISR method in IRS, peak signal-to-noise ratio (PSNR)[50] and structural similarity index measure (SSIM)[51] can be used besides the subjective visual appearance.

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \tag{9}$$

$$MSE = \frac{\left(\sum_{i=1}^{m}\sum_{j=1}^{n}\left(I_o(i,j)-I_r(i,j)\right)^2\right)}{m\times n} \tag{10}$$

$$SSIM = \frac{(2\mu_o u_r + c_1)(2\sigma_{or} + c_2)}{(\mu_o^2 + \mu_r^2 + c_1)(\sigma_o^2 + \sigma_r^2 + c_2)} \tag{11}$$

Where, I_o and I_r are the original and the reconstructed images, respectively; m and n are the height and width of the image; μ_o and μ_r are mean intensities of images (original and reconstructed images); σ_o , and σ_r represent the standard deviation of original and reconstructed image, respectively; σ_{or} is the covariance of images; $c1$ and $c2$ are constants that $c1$ is 0.01 and $c2$ is 0.03.

4-2- Experimental Results

In these experiments, the algorithm parameters are selected as constant in order to prevent the selection of the parameters' values from affecting the results of SR process (Table 1). The test and training sets are completely non-overlapped. For HR images, the patch size and overlap between patches are set to 16 × 16 and 12 pixels, respectively. Similarly, it is set to 4×4 and 3 pixels, respectively, for LR images. Four sets of tests are done as follows: The qualitative performance of the proposed method is checked in the first set; the quantitative performance of the proposed method is examined in the second set; and the performance of other meta-heuristic algorithms for the SR process is examined in the third set. The performance of the proposed method is checked on different databases in the fourth set.

Table 1. Parameter values in different methods

Algorithm	Parameters	Value
GWO[19]	a	2 to 0
	Population size	100
	Maximum iteration	100
NE[46]	K	12
Sparse Neighbor Embedding[46]	δ_{min}	0.0001
	η	4
	b	0.9
FA	γ	1
	β_0	1
	α	0 to 1

PSO[19]	w	0.9 to 0.2
	c_1	2 to 0
	c_2	0 to 2
	Population size	100
	Maximum iterations	100
GSA[52]	α	5
	G_0	100
	c_1	2 to 0.1
	c_2	0 to 1
	Population size	100
	Maximum iterations	100
GOA	Population size	100
	Maximum iteration	100
GOA-ISR	Population size	100
	Maximum iteration	100
	λ_1	0.8
	λ_2	0.1

4-2-1- Qualitative Investigation of the Proposed GOA-ISR Method Performance

In this experiment, natural images [44] are used to qualitatively check the performance of the proposed GOA-ISR method in the SR process, and an example of SR results using the proposed method is shown in Fig. 3.



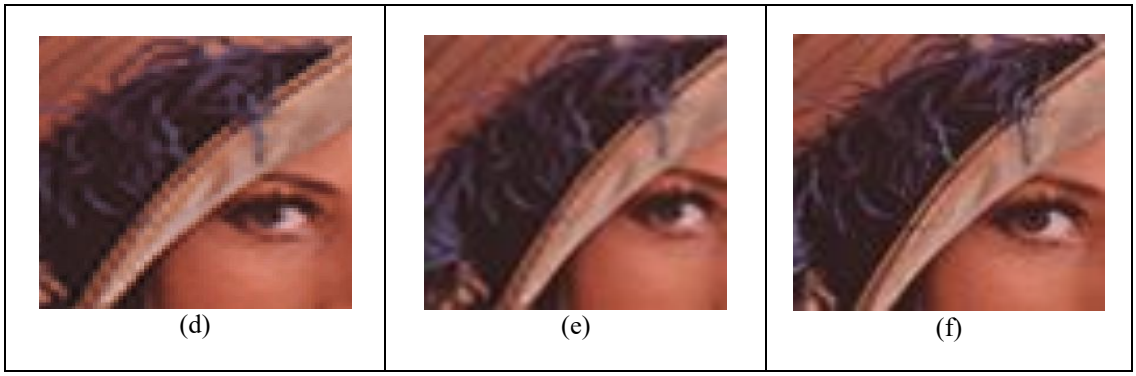


Fig. 3. Results of different methods of SR process, (a) Bicubic[9] (RMSE=4.18),(b) NE [43] (RMSE=4.23), (c) SC[44] (RMSE=4.03), (d) IKC [45] (RMSE=3.52), (e) Proposed GOA-ISR method (RMSE=3.21) (f) Ground truth

As shown in Fig. 3, the SR process in the Bicubic and NE methods has created artifact edges, while the SC method has caused the removal of sharp edges and blurring. IKC method has fewer artifact edges than Bicubic and NE methods, and thus, this method performs better than the Bicubic and NE methods in the SR process. Sharp edges in the proposed GOA-ISR method are recovered better than in other methods and have much clearer details with less artifacts. The image of the proposed GOA-ISR method is very close to the ground truth image, which indicates the proper performance of the proposed method.

4-2-2- Quantitative Investigation of the Proposed GOA-ISR Method Performance

In this experiment, 20 images from the DVI2K database were used to check the quantitative performance of the proposed GOA-ISR method, and the results are shown in Table 2.

Table 2. Quantitative results of SR methods

IMAGE	**Sparse Neighbor Embedding[46]**	**Adaptive Sparse[47]**	**GWO[19]**	**SAN[48]**	**DWSR[53]**	**Proposed GOA-ISR method**
	PSNR(dB) SSIM	PSNR (dB) SSIM	PSNR (dB) SSIM	PSNR (dB) SSIM	PSNR (dB) SSIM	PSNR (dB) SSIM
Image 1	19.44 0.691	26.37 0.821	27.31 0.801	31.10 0.890	32.20 0.897	**34.72 0.945**
Image 2	17.84 0.704	20.24 0.685	23.40 0.806	26.91 0.831	28.37 0.871	**32.56 0.923**
Image 3	21.52 0.715	26.11 0.847	25.16 0.812	28.53 0.834	26.08 0.786	**31.87 0.909**
Image 4	17.81 0.702	24.71 0.834	24.02 0.791	29.09 0.856	33.11 0.905	**34.39 0.934**
Image 5	16.61 0.566	21.42 0.739	21.75 0.725	27.30 0.871	32.42 0.930	**34.33 0.935**
Image 6	19.89 0.722	26.89 0.813	25.63 0.835	28.38 0.835	32.24 0.896	**35.32 0.940**
Image 7	18.78 0.706	22.87 0.835	24.74 0.829	27.75 0.845	32.84 0.891	**34.96 0.925**
Image 8	20.81 0.714	23.30 0.833	25.72 0.823	28.24 0.847	29.75 0.90	**33.23 0.926**
Image 9	21.63 0.736	27.73 0.848	28.45 0.837	31.13 0.897	32.48 0.92	**33.0 5 0.933**
Image 10	20.90 0.7303	23.45 0.821	27.23 0.849	28.49 0.869	31.54 0.88	**33.89 0.939**
Image 11	17.28 0.651	22.83 0.811	22.78 0.786	28.45 0.837	32.23 0.896	**34.40 0.929**
Image 12	16.58 0.645	22.61 0.810	21.94 0.772	27.86 0.842	32.02 0.893	**33.89 0.931**
Image 13	19.37 0.716	25.17 0.806	25.12 0.830	28.05 0.835	28.74 0.857	**31.74 0.913**
Image 14	20.48 0.675	26.09 0.830	25.84 0.798	21.74 0.690	29.17 0.843	**31.45 0.917**
Image 15	26.00 0.702	25.96 0.667	23.14 0.657	24.52 0.722	31.35 0.883	**32.49 0.931**
Image 16	20.87 0.628	24.23 0.821	22.31 0.812	23.61 0.718	30.69 0.910	**32.83 0.925**
Image 17	21.20 0.723	27.24 0.850	26.84 0.855	28.06 0.846	29.09 0.889	**33.60 0.938**
Image 18	18.02 0.691	20.31 0.791	22.34 0.762	25.03 0.763	30.38 0.786	**32.19 0.873**
Image 19	19.31 0.701	24.03 0.892	23.62 0.780	26.82 0.820	28.01 0.871	**29.34 0.908**
Image 20	17.98 0.618	23.79 0.810	24.05 0.742	28.49 0.858	29.21 0.861	**34.38 0.943**

As seen in Table 2, the sparse neighbor embedding method has a weaker performance than the other methods, but the GWO and SAN methods have an acceptable performance in the SR process. The quantitative evaluation results show that the performance of the proposed GOA-ISR method is better than other methods, such as the SAN method.

4-2-3- Investigating Other Meta-Heuristic Algorithms in the SR Process

In this test, other meta-heuristic algorithms, such as Particle Swarm Optimization (PSO) and Gravitational Search Algorithm (GSA), and Firefly Algorithm (FA) are used to recover the weight value in the SR process. The DVI2K database is used in this study.

Table 3. The results of the SR process on meta-heuristic algorithms

Algorithms	PSNR(dB)
PSO	16.23

GSA	18.71
FA	19.08
GOA	22.43
Proposed GOA-ISR Method	**24.19**

As seen in Table 3, the value of PSNR in GOA and the proposed GOA-ISR methods are better than that in other meta-heuristic algorithms, such as PSO, GSA, and FA. The effective and better performance of this algorithm has been proven against other meta-heuristic algorithms [54]. The reason that the performance of the proposed GOA-ISR method is better than the classic GOA is that the search space in the proposed GOA-ISR method is limited, and the local optimum is prevented from getting stuck by providing upper bound and lower bound formulas.

4-2-4- Checking the Proposed GOA-ISR Method on Other Databases

In this experiment, URBAN100 [55], BSD100[56], Set 14 [57] and Set 5 [28]databases were used to evaluate the performance of the proposed GOA-ISR method, and the results are shown in Fig 4 and Table 4.

Table 4. Performance evaluation of the proposed GOA-ISR method on different databases

Database	Average PSNR
URBAN100	26.43
BSD100	27.65
Set 14	31.24
Set 5	30.09

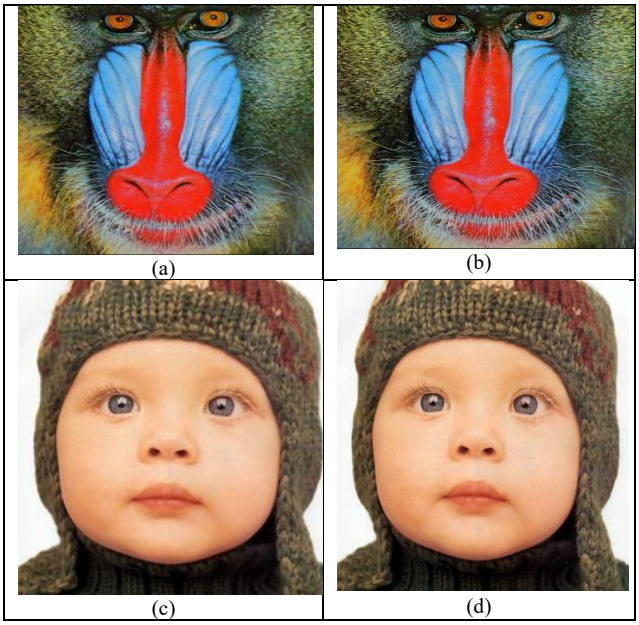


Fig. 4. The results of the SR process, (a)(c) HR image ,(b)(d) Proposed GOA-ISR method

The images of the proposed GOA-ISR method are very close to the HR images, which indicates the proper performance of the proposed GOA-ISR method (Fig. 4).

5- Conclusion

In this study, a new approach based on the GOA is proposed to obtain optimal reconstruction weights in the ISR process. The suggested GOA-ISR obtains optimal reconstruction weights for training LR images, which leads to promising reconstruction of HR images. In this approach, the distances between the training patches and input are calculated, so the performance of the SR process can be better compared with the classical GOA algorithm. In the future studies, it will be tried to achieve the maximum improvement of the SR process through using a suitable method to optimize the fixed parameters of the algorithm, that is, instead of the trial and error method, the parameters of the algorithm should be obtained systematically.

References

[1] B. Ghaderi and H. Azad, "Deep Learning Algorithms in Super-Resolution Images," Journal of Circuits, Data and Systems Analysis, vol. 1, no. 1, p. 47, 2023.

[2] P. Behjati, P. Rodriguez, C. Fernández, I. Hupont, A. Mehri, and J. Gonzàlez, "Single image super-resolution based on directional variance attention network," Pattern Recognition, vol. 133, p. 108997, 2023.

[3] T. Goto, T. Fukuoka, F. Nagashima, S. Hirano, and M. Sakurai, "Super-resolution System for 4K-HDTV," in 2014 22nd International Conference on Pattern Recognition, 2014: IEEE, pp. 4453-4458.

[4] A. Rapuano, G. Iovane, and M. Chinnici, "A scalable Blockchain based system for super resolution images manipulation," in 2020 IEEE 6th International Conference on Dependability in Sensor, Cloud and Big Data Systems and Application (DependSys), 2020: IEEE, pp. 8-15.

[5] H. Dastmalchi and H. Aghaeinia, "Super-resolution of very low-resolution face images with a wavelet integrated, identity preserving, adversarial network," Signal Processing: Image Communication, p. 116755, 2022.

[6] I. Taghavi et al., "Ultrasound super-resolution imaging with a hierarchical Kalman tracker," Ultrasonics, vol. 122, p. 106695, 2022.

[7] P. Wang, B. Bayram, and E. Sertel, "A comprehensive review on deep learning based remote sensing image super-resolution methods," Earth-Science Reviews, p. 104110, 2022.

[8] K. Zhu, H. Guo, S. Li, and X. Lin, "Online tool wear monitoring by super-resolution based machine vision," Computers in Industry, vol. 144, p. 103782, 2023.

[9] H. Hou and H. Andrews, "Cubic splines for image interpolation and digital filtering," IEEE Transactions on acoustics, speech, and signal processing, vol. 26, no. 6, pp. 508-517, 1978.

[10] M. Li and T. Q. Nguyen, "Markov random field model-based edge-directed image interpolation," IEEE Transactions on Image Processing, vol. 17, no. 7, pp. 1121-1128, 2008.

[11] J. Sun, J. Zhu, and M. F. Tappen, "Context-constrained hallucination for image super-resolution," in 2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2010: IEEE, pp. 231-238.
[12] L. Wang, S. Xiang, G. Meng, H. Wu, and C. Pan, "Edge-directed single-image super-resolution via adaptive gradient magnitude self-interpolation," IEEE Transactions on Circuits and Systems for Video Technology, vol. 23, no. 8, pp. 1289-1299, 2013.
[13] W. T. Freeman, T. R. Jones, and E. C. Pasztor, "Example-based super-resolution," IEEE Computer graphics and Applications, vol. 22, no. 2, pp. 56-65, 2002.
[14] C. Dong, C. C. Loy, K. He, and X. Tang, "Learning a deep convolutional network for image super-resolution," in European conference on computer vision, 2014: Springer, pp. 184-199.
[15] K. Zhang, J. Li, H. Wang, X. Liu, and X. Gao, "Learning local dictionaries and similarity structures for single image super-resolution," Signal Processing, vol. 142, pp. 231-243, 2018.
[16] N. Kumar and A. Sethi, "Fast learning-based single image super-resolution," IEEE Transactions on Multimedia, vol. 18, no. 8, pp. 1504-1515, 2016.
[17] J. Jiang, C. Wang, X. Liu, and J. Ma, "Deep learning-based face super-resolution: A survey," ACM Computing Surveys (CSUR), vol. 55, no. 1, pp. 1-36, 2021.
[18] P. P. Gajjar and M. V. Joshi, "New learning based super-resolution: use of DWT and IGMRF prior," IEEE Transactions on Image Processing, vol. 19, no. 5, pp. 1201-1213, 2010.
[19] S. S. Rajput, V. K. Bohat, and K. Arya, "Grey wolf optimization algorithm for facial image super-resolution," Applied Intelligence, vol. 49, no. 4, pp. 1324-1338, 2019.
[20] K. Nguyen, C. Fookes, S. Sridharan, M. Tistarelli, and M. Nixon, "Super-resolution for biometrics: A comprehensive survey," Pattern Recognition, vol. 78, pp. 23-42, 2018.
[21] N. Wang, D. Tao, X. Gao, X. Li, and J. Li, "A comprehensive survey to face hallucination," International journal of computer vision, vol. 106, no. 1, pp. 9-30, 2014.
[22] Y. Tang, P. Yan, Y. Yuan, and X. Li, "Single-image super-resolution via local learning," International Journal of Machine Learning and Cybernetics, vol. 2, no. 1, pp. 15-23, 2011.
[23] K. Zhang, X. Gao, D. Tao, and X. Li, "Single image super-resolution with non-local means and steering kernel regression," IEEE Transactions on Image Processing, vol. 21, no. 11, pp. 4544-4556, 2012.
[24] K. Zhang, X. Gao, D. Tao, and X. Li, "Single image super-resolution with multiscale similarity learning," IEEE transactions on neural networks and learning systems, vol. 24, no. 10, pp. 1648-1659, 2013.
[25] Z. Wang, Y. Yang, Z. Wang, S. Chang, J. Yang, and T. S. Huang, "Learning super-resolution jointly from external and internal examples," IEEE Transactions on Image Processing, vol. 24, no. 11, pp. 4359-4371, 2015.
[26] X. Lu, H. Yuan, Y. Yuan, P. Yan, L. Li, and X. Li, "Local learning-based image super-resolution," in 2011 IEEE 13th International Workshop on Multimedia Signal Processing, 2011: IEEE, pp. 1-5.
[27] L. An and B. Bhanu, "Image super-resolution by extreme learning machine," in 2012 19th IEEE international conference on image processing, 2012: IEEE, pp. 2209-2212.
[28] M. Bevilacqua, A. Roumy, C. Guillemot, and M. L. Alberi-Morel, "Low-complexity single-image super-resolution based on nonnegative neighbor embedding," 2012.
[29] S. Saremi, S. Mirjalili, and A. Lewis, "Grasshopper optimisation algorithm: theory and application," Advances in engineering software, vol. 105, pp. 30-47, 2017.
[30] I. J. Cox, M. L. Miller, J. A. Bloom, and C. Honsinger, Digital watermarking. Springer, 2002.
[31] P. Tumuluru and B. Ravi, "GOA-based DBN: Grasshopper optimization algorithm-based deep belief neural networks for cancer classification," International Journal of Applied Engineering Research, vol. 12, no. 24, pp. 14218-14231, 2017.
[32] P.-H. Dinh, "A novel approach based on grasshopper optimization algorithm for medical image fusion," Expert Systems with Applications, vol. 171, p. 114576, 2021.
[33] J. H. Holland, "Genetic algorithms," Scientific american, vol. 267, no. 1, pp. 66-73, 1992.
[34] R. Eberhart and J. Kennedy, "A new optimizer using particle swarm theory," in MHS'95. Proceedings of the sixth international symposium on micro machine and human science, 1995: Ieee, pp. 39-43.
[35] A. Kamalinia and A. Ghaffari, "Hybrid task scheduling method for cloud computing by genetic and PSO algorithms," J. Inf. Syst. Telecommun, vol. 4, pp. 271-281, 2016.
[36] X.-S. Yang, "Firefly algorithms for multimodal optimization," in International symposium on stochastic algorithms, 2009: Springer, pp. 169-178.
[37] A. Mahmoodzadeh, H. Agahi, and M. Salehi, "Handwritten Digits Recognition Using an Ensemble Technique Based on the Firefly Algorithm," Journal of Information Systems and Telecommunication (JIST), vol. 3, no. 23, p. 136, 2019.
[38] X.-S. Yang, "A new metaheuristic bat-inspired algorithm," in Nature inspired cooperative strategies for optimization (NICSO 2010): Springer, 2010, pp. 65-74.
[39] E. Rashedi, E. Rashedi, and H. Nezamabadi-Pour, "A comprehensive survey on gravitational search algorithm," Swarm and evolutionary computation, vol. 41, pp. 141-158, 2018.
[40] M. Tourani, "Improvement of Firefly Algorithm using Particle Swarm Optimization and Gravitational Search Algorithm," Journal of Information Systems and Telecommunication (JIST), vol. 2, no. 34, p. 123, 2021.
[41] C. M. Topaz, A. J. Bernoff, S. Logan, and W. Toolson, "A model for rolling swarms of locusts," The European Physical Journal Special Topics, vol. 157, no. 1, pp. 93-109, 2008.
[42] S. M. Rogers, T. Matheson, E. Despland, T. Dodgson, M. Burrows, and S. J. Simpson, "Mechanosensory-induced behavioural gregarization in the desert locust Schistocerca gregaria," Journal of Experimental Biology, vol. 206, no. 22, pp. 3991-4002, 2003.
[43]Y. ChangH, "XiongY. Super-resolutionthroughneighborembedding," Proceedingsofthe2004IEEEComputer Society C o nference on ComputerVision and Pattern Rec ogni—tion, pp. 275-282, 2004.
[44]J. Yang, J. Wright, T. S. Huang, and Y. Ma, "Image super-resolution via sparse representation," IEEE transactions on image processing, vol. 19, no. 11, pp. 2861-2873, 2010.
[45]J. Gu, H. Lu, W. Zuo, and C. Dong, "Blind super-resolution with iterative kernel correction," in Proceedings of the

IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2019, pp. 1604-1613.

[46] X. Gao, K. Zhang, D. Tao, and X. Li, "Image super-resolution with sparse neighbor embedding," IEEE Transactions on Image Processing, vol. 21, no. 7, pp. 3194-3205, 2012.

[47] W. Dong, L. Zhang, G. Shi, and X. Wu, "Image deblurring and super-resolution by adaptive sparse domain selection and adaptive regularization," IEEE Transactions on image processing, vol. 20, no. 7, pp. 1838-1857, 2011.

[48] T. Dai, J. Cai, Y. Zhang, S.-T. Xia, and L. Zhang, "Second-order attention network for single image super-resolution," in Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, 2019, pp. 11065-11074.

[49] E. Agustsson and R. Timofte, "Ntire 2017 challenge on single image super-resolution: Dataset and study," in Proceedings of the IEEE conference on computer vision and pattern recognition workshops, 2017, pp. 126-135.

[50] F. Akhlaghian Tab, K. Ghaderi, and P. Moradi, "A New Robust Digital Image Watermarking Algorithm Based on LWT-SVD and Fractal Images," Journal of Information Systems and Telecommunication (JIST), vol. 1, no. 9, p. 1, 2015.

[51] K. Li, S. Yang, R. Dong, X. Wang, and J. Huang, "Survey of single image super-resolution reconstruction," IET Image Processing, vol. 14, no. 11, pp. 2273-2290, 2020.

[52] V. K. Bohat and K. Arya, "An effective gbest-guided gravitational search algorithm for real-parameter optimization and its application in training of feedforward neural networks," Knowledge-Based Systems, vol. 143, pp. 192-207, 2018.

[53] S.-C. Chu, Z.-C. Dou, J.-S. Pan, L. Kong, V. Snášel, and J. Watada, "DWSR: an architecture optimization framework for adaptive super-resolution neural networks based on meta-heuristics," Artificial Intelligence Review, vol. 57, no. 2, p. 23, 2024.

[54] Y. Meraihi, A. B. Gabis, S. Mirjalili, and A. Ramdane-Cherif, "Grasshopper optimization algorithm: theory, variants, and applications," IEEE Access, vol. 9, pp. 50001-50024, 2021.

[55] J.-B. Huang, A. Singh, and N. Ahuja, "Single image super-resolution from transformed self-exemplars," in Proceedings of the IEEE conference on computer vision and pattern recognition, 2015, pp. 5197-5206.

[56] D. Martin, C. Fowlkes, D. Tal, and J. Malik, "A database of human segmented natural images and its application to evaluating segmentation algorithms and measuring ecological statistics," in Proceedings eighth IEEE international conference on computer vision. ICCV 2001, 2001, vol. 2: IEEE, pp. 416-423.

[57] R. Zeyde, M. Elad, and M. Protter, "On single image scale-up using sparse-representations," in Curves and Surfaces: 7th International Conference, Avignon, France, June 24-30, 2010, Revised Selected Papers 7, 2012: Springer, pp. 711-730.