Cost-Effective Strategy for IIoT Security based on Bi-Objective Optimization

Sofiane HAMRIOUI * † ||, Pascal LORENZ †, Jaime LLORET ‡ and Joel J. P. C RODRIGUES §

***Abstract*—The Internet of Things (IoT) and its industrial counterpart, the Industrial Internet of Things (IIoT), have transformed sectors such as home automation, healthcare, and manufacturing by enhancing data management through advanced networking. However, the rapid growth of IIoT has introduced significant cybersecurity challenges, necessitating a comprehensive approach to securing data across the TCP/IP model. This paper presents a novel cybersecurity investment strategy formulated as a bi-objective optimization problem, validated through genetic and iterative algorithms. The strategy effectively balances security and cost, achieving nearly 50% efficiency in solution effectiveness. By utilizing these optimization techniques, the approach provides a practical and cost-effective solution to improve IIoT security within budget constraints, offering valuable insights for cybersecurity professionals seeking robust and economically viable solutions.**

***Index Terms*—IIoT, Cybersecurity, TCP/IP Layers, Optimization Approach, Bi-Objective Optimization, Genetic Algorithms, Iterative Algorithms, Cost-Effective Security.**

I. Introduction

Recently, the Industrial Internet of Things (IIoT) has become pivotal in advancing industrial processes such as manufacturing, predictive maintenance, and supply chain management, with industry leaders like General Electric and Siemens driving the Industry 4.0 revolution [1]–[4]. However, the increased connectivity in IIoT systems also amplifies cybersecurity risks, as highlighted by incidents such as the 2017 WannaCry ransomware attack [5]. These threats underscore the growing vulnerability of critical infrastructures, making the need for robust and adaptive cybersecurity solutions for IIoT environments more urgent than ever. Securing IIoT systems requires addressing vulnerabilities across multiple layers, from physical devices and sensors to communication networks and control mechanisms. Common threats include environmental risks for sensors, MAC flooding and DDoS attacks at the data link layer, TCP and UDP floods at the transport layer, and FTP bounce attacks and code injection at the application layer. As such, an effective security strategy must encompass continuous monitoring, real-time threat detection, and adaptive defenses, all while balancing performance, reliability, and cost-efficiency. Given the evolving nature of cyber threats, IIoT systems require a proactive, layered security approach that optimizes protection and resource allocation within financial constraints.

This paper introduces a novel bi-objective optimization framework for cybersecurity investments tailored to IIoT environments. The framework simultaneously maximizes security (ensuring confidentiality, integrity, and availability) and minimizes costs associated with implementing security measures. Specifically, the framework formulates security investment as a trade-off between these two objectives, using Pareto-based trade-off analysis to identify a set of optimal solutions. Each solution represents an efficient allocation of resources that balances security improvements with budgetary constraints. Our approach addresses the unique challenges of IIoT systems, which are critical to industrial operations and require adaptive, cost-effective security solutions. The core innovation of our method, detailed in Section 3, lies in its ability to identify optimal security investment strategies across the access, network, and application layers, providing a systematic way to mitigate threats while adhering to budgetary constraints. Our experimental results demonstrate the competitiveness and efficacy of our approach compared to existing techniques, showing significant improvements in both security performance and cost efficiency. This positions our solution as a robust, economically viable defense mechanism suitable for real-world industrial applications.

The remainder of this paper is structured as follows: Section 2 reviews related research on IoT and IIoT cybersecurity. Section 3 formalizes the bi-objective optimization problem and presents the proposed solution. Section 4 is devoted to the experimental analysis and comparative evaluation. Finally, Section 5 concludes with key findings and future research directions.

II. Related Works

Cybersecurity in IoT and IIoT systems is typically categorized into two key areas: vulnerability analysis and cost-effective security strategies. Vulnerabilities related to communication and device integrity are discussed by [7] and [8], which emphasize concerns such as unauthorized access and data breaches. Evolving threats, including Advanced Persistent Threats (APTs) and zero-day vulnerabilities, are explored by [9], while [10] advocates for enhanced encryption and authentication techniques in smart homes. Cost-effective strategies are further explored by [11], who proposes fog computing as a means to decentralize data and improve security. Additionally, [12] introduces low-cost authentication methods, and [13] and [14] focus on efficient cryptographic approaches. Machine learning techniques for anomaly detection are applied by [15],

* CERADE, ESAIP Engineer School, Saint Barthélemy d'Anjou, France
† IRIMAS, Haute Alsace University, Mulhouse-Colmar, France
‡ Universitat Politecnica de Valencia, Valencia, Spain
§ Federal University of Piauí (UFPI), Teresina - PI, Brazil
|| PARAGRAPHE, Paris 8 University, St Denis, France
E-mails : shamrioui@esaip.org, lorenz@ieee.org, jlloret@dcom.upv.es, joeljr@ieee.org

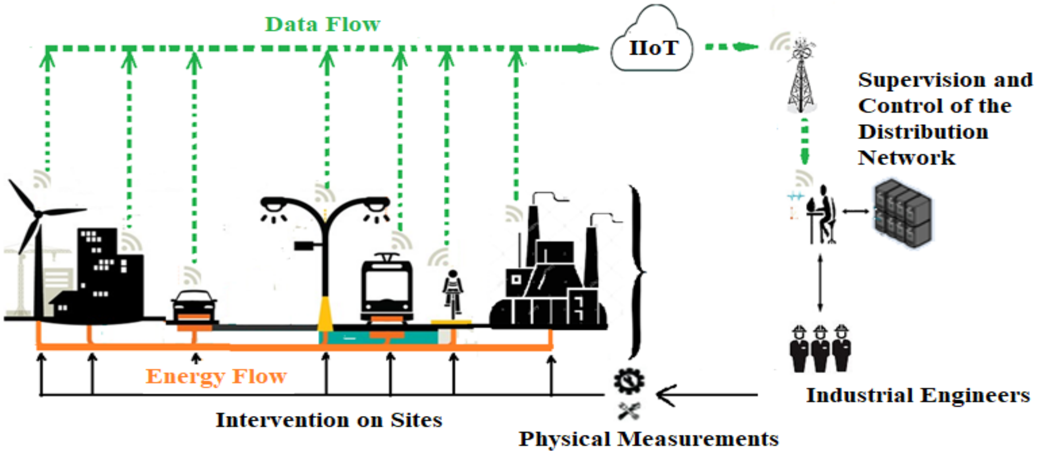

Fig. 1. IIoT Application for Energy Management System

while [16] suggests the use of blockchain for securing decentralized transactions. Collectively, these studies underscore the growing demand for affordable, effective security solutions in the IIoT domain.

However, bi-objective optimization in IIoT security remains an emerging field. Recent studies, such as [17] and [18], address the challenge of security-resource constraints, while [19] and [20] focus on balancing security with cost. Nonetheless, these approaches often fail to account for the multi-layered nature of IIoT systems. In recent years, bi-objective optimization has gained significant attention. For example, [21] introduced a Length-Adaptive Genetic Algorithm for Bi-Objective High-Dimensional Feature Selection, which is particularly useful in complex environments like IIoT, where multiple objectives need to be balanced. Similarly, [22] proposed a Multi-Swarm Co-Evolution Hybrid Optimization approach for Bi-Objective Multi-Workflow Scheduling, which could be applied to IIoT systems, where efficient resource allocation and time optimization are critical. Studies such as [23] on Biobjective Robust Incentive Mechanism Design and [24] on Biobjective Task Scheduling in Green Cloud Data Centers focus on optimizing conflicting objectives under uncertainty. Although these approaches target different domains, they provide valuable insights into optimizing resource allocation and security in IIoT systems.

Our approach differs by addressing the unique security challenges of IIoT systems, including multi-layer security and dynamic investment strategies to balance cyber threats and budget constraints. Unlike [23] and [24], which focus on resource allocation in crowdsourcing and cloud environments, our model is specifically tailored to IIoT systems, optimizing security investments across multiple layers to ensure comprehensive and cost-effective protection. While previous studies provide useful insights into vulnerabilities and cost-effective solutions, they often fail to address the evolving nature of threats or the prioritization of security investments. Our proposed bi-objective optimization strategy balances security and budget constraints, offering a dynamic, cost-efficient solution for the evolving needs of IIoT systems.

III. The Proposed Cost-Effective Strategy

Integrating IoT into industrial processes requires managing data flow across multiple communication layers. In IIoT energy management systems, for example (see Figure 1), optimizing energy use and operational efficiency is critical but must be balanced with robust security and cost control. Given the critical nature of IIoT infrastructure, cybersecurity risks threaten both efficiency and integrity. The proposed strategy employs a bi-objective optimization approach to maximize the global security level (S) of a given IIoT environment while minimizing the necessary global cost (C) to get (S). Each layer—access, network, and application—faces unique vulnerabilities and cost factors. Security parameters for layer i, denoted as S_i, encompass confidentiality, integrity, and availability (CIA), defined within flexible ranges $[\underline{S_i}, \overline{S_i}]$, allowing for adjustments based on evolving threats and risk profiles specific to each layer. This dynamic adaptation is crucial since cybersecurity threats are rarely static. Similarly, cost parameters (C_i) are bounded by $[\underline{C_i}, \overline{C_i}]$, ensuring that security investments remain within budget constraints. This approach emphasizes flexibility in resource allocation while maintaining optimal security, reflecting the cost-efficiency and adaptability required in real-world IIoT scenarios [25].

Moreover, the approach uses an adaptive strategy that allows for real-time re-evaluation of investment priorities, ensuring that the solution remains aligned with changing security needs and budget constraints. This continuous adaptation enhances the resilience of the system against emerging threats. Although this model can be applied to scenarios where both performance and cost optimization are important, it is specifically adapted for IIoT environments. The unique integration of communication layers and dynamic threat assessment tailored to IIoT's operational needs sets it apart, ensuring that security investments align with real-time risk analysis and system priorities. This model supports effective decision-making in contexts where IIoT's security and operational performance are at stake, providing a balance that may not be achieved in broader optimization models.

In this approach, the dynamic nature of security requirements is addressed by parameterizing the S_i and C_i values as a range, capturing the evolving trade-off between security levels

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2025.3525779

TABLE I
TABLE OF SYMBOLS FOR IIOT SECURITY INVESTMENT OPTIMIZATION

Symbol	Description
$\mathbf{n}$	Number of communication layers considered
$\mathbf{S_i}$	Security objective for layer $\mathbf{i}$
$\mathbf{S_{Vi}}$	Security weighting vector: $\mathbf{S_{Vi}} = (\mathbf{S_{Vi1}}, \mathbf{S_{Vi2}}, \mathbf{S_{Vi3}})$
$\mathbf{S_{Vi1}}$	Security weighting for confidentiality at layer $\mathbf{i}$
$\mathbf{S_{Vi2}}$	Security weighting for integrity at layer $\mathbf{i}$
$\mathbf{S_{Vi3}}$	Security weighting for availability at layer $\mathbf{i}$
$\mathbf{X_{i1}}$	Confidentiality level at layer $\mathbf{i}$
$\mathbf{X_{i2}}$	Integrity level at layer $\mathbf{i}$
$\mathbf{X_{i3}}$	Availability level at layer $\mathbf{i}$
$\mathbf{Y_i}$	Cost vector: $\mathbf{Y_i} = (\mathbf{Y_{i1}}, \mathbf{Y_{i2}}, \mathbf{Y_{i3}})$
$\mathbf{Y_{i1}}$	Cost for confidentiality at layer $\mathbf{i}$
$\mathbf{Y_{i2}}$	Cost for integrity at layer $\mathbf{i}$
$\mathbf{Y_{i3}}$	Cost for availability at layer $\mathbf{i}$
$\mathbf{C_{Vi}}$	Cost weighting vector: $\mathbf{C_{Vi}} = (\mathbf{C_{Vi1}}, \mathbf{C_{Vi2}}, \mathbf{C_{Vi3}})$
$\mathbf{C_{Vi1}}$	Cost weighting for confidentiality at layer $\mathbf{i}$
$\mathbf{C_{Vi2}}$	Cost weighting for integrity at layer $\mathbf{i}$
$\mathbf{C_{Vi3}}$	Cost weighting for availability at layer $\mathbf{i}$
$\mathbf{C_i}$	Cost objective for layer $\mathbf{i}$
$\underline{\mathbf{S_i}}$	Lower bound of the security level for layer $\mathbf{i}$
$\overline{\mathbf{S_i}}$	Upper bound of the security level for layer $\mathbf{i}$
$\underline{\mathbf{C_i}}$	Lower bound of the budget for layer $\mathbf{i}$
$\overline{\mathbf{C_i}}$	Upper bound of the budget for layer $\mathbf{i}$
$\mathbf{K}$	Maximum number of layers eligible for investment

and investment costs. The bi-objective optimization model is formulated using two systems of inequalities, $Syst_{Security}$ and $Syst_{Cost}$, as shown in equations (1) and (2). These systems optimize cybersecurity investments across the access, network, and application layers. The $Syst_{Security}$ system ensures that security requirements related to confidentiality, integrity, and availability are met, while the $Syst_{Cost}$ system ensures that costs remain within budget. This dual-objective model balances security and financial constraints, facilitating efficient resource allocation. The bi-objective model is designed to dynamically prioritize the most critical layers based on the real-time analysis of threat intelligence and system performance metrics, which helps to adapt the strategy to current and future risks.

$$Syst_{Security} = \left\{ \begin{array}{lcl} S_{V11}X_{11} + S_{V12}X_{12} + S_{V13}X_{13} & \geq & S_1 \\ S_{V21}X_{21} + S_{V22}X_{22} + S_{V23}X_{23} & \geq & S_2 \\ S_{V31}X_{31} + S_{V32}X_{32} + S_{V33}X_{33} & \geq & S_3 \end{array} \right.$$

subject to:

$$\left\{ \begin{array}{l} K = 3 \\ \sum_{i=1}^{K} S_i = S \\ X_{i1} \geq 0,\ X_{i2} \geq 0,\ X_{i3} \geq 0 \\ S_i \in [\underline{S_i}, \overline{S_i}],\ i = 1, \ldots, 3 \end{array} \right. \tag{1}$$

$$Syst_{Cost} = \left\{ \begin{array}{lcl} C_{V11}Y_{11} + C_{V12}Y_{12} + C_{V13}Y_{13} & \leq & C_1 \\ C_{V21}Y_{21} + C_{V22}Y_{22} + C_{V23}Y_{23} & \leq & C_2 \\ C_{V31}Y_{31} + C_{V32}Y_{32} + C_{V33}Y_{33} & \leq & C_3 \end{array} \right.$$

subject to:

$$\left\{ \begin{array}{l} K = 3 \\ \sum_{i=1}^{K} C_i = C \\ Y_{i1} \geq 0,\ Y_{i2} \geq 0,\ Y_{i3} \geq 0 \\ C_i \in [\underline{C_i}, \overline{C_i}],\ i = 1, \ldots, 3 \end{array} \right. \tag{2}$$

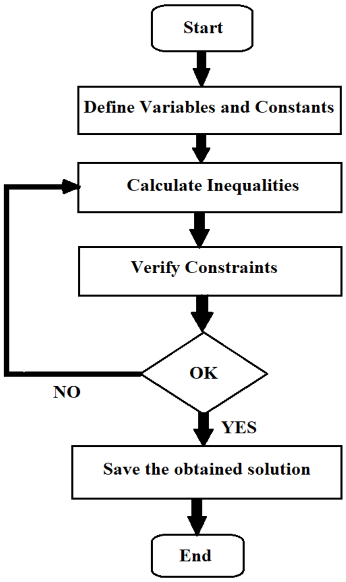

Fig. 2. Main steps of the proposed cybersecurity strategy

The strategy employs fuzzy and probabilistic modeling to account for the dynamic nature of security levels S_i, with deterministic models treating S_i as a range $[\underline{S_i}, \overline{S_i}]$. Fuzzy logic reflects the inherent uncertainties in threat detection and vulnerability assessments, which are imprecise and dynamic. Additionally, a limit K restricts investments to a subset of communication layers, optimizing resource allocation within budget constraints and aligning with portfolio management principles [25]. This incorporation of fuzzy and probabilistic modeling ensures that the strategy can handle ambiguity and variability in threat landscape assessments, leading to more robust decision-making. The table I provides a summary of the different symbols and their corresponding descriptions, used while formulating the proposed approach.

The flow chart in Figure 2 illustrates the process for optimizing cybersecurity investments in IIoT systems. This process aligns security needs with budget constraints, driven by the dual objectives $Systy_{Security}$ and $Syst_{Costy}$. To optimize investments, the decision-making process focuses on identifying critical communication layers—access, network, and application—each characterized by distinct vulnerabilities. Security needs are evaluated using $Systy_{Security}$ inequalities, focusing on the CIA triad, while costs are assessed with $Syst_{Costy}$ inequalities to balance security and financial efficiency. Layer prioritization is managed using constraint K, limiting the number of layers considered. The process includes continuous review and adjustment of security measures and budgets to adapt to evolving threats, ensuring the plan is implemented within budget. This methodology provides a structured approach to balancing security with financial constraints, offering clear and strategic insights.

To address the optimization problem, we use two key matrices. The first matrix, M_S, defined in equation (3), captures the security triad by setting lower bounds for the minimum security requirements of each critical layer, denoted as X_{i1}, X_{i2}, and X_{i3} for $i = 1, \ldots, 3$. These elements represent the required security levels for confidentiality (X_{i1}), integrity

(X_{i2}), and availability (X_{i3}) for each layer i. The second matrix, M_C, defined in equation (4), outlines cost constraints by providing upper bounds for the maximum allowable costs, represented by Y_{i1}, Y_{i2}, and Y_{i3}. These elements correspond to the costs for achieving the required levels of confidentiality (Y_{i1}), integrity (Y_{i2}), and availability (Y_{i3}) at each layer i. Together, M_S and M_C establish feasible security and cost parameters, enabling effective balancing of security needs with budget constraints to optimize cybersecurity investments.

$$M_S = \begin{bmatrix} X_{11} & X_{12} & X_{13} \\ X_{21} & X_{22} & X_{23} \\ X_{31} & X_{32} & X_{33} \end{bmatrix} \tag{3}$$

$$M_C = \begin{bmatrix} Y_{11} & Y_{12} & Y_{13} \\ Y_{21} & Y_{22} & Y_{23} \\ Y_{31} & Y_{32} & Y_{33} \end{bmatrix} \tag{4}$$

IV. COMPUTATIONAL RESULTS AND ANALYSIS

A. Simulation Environment and Parameters

To solve the optimization problem, the study evaluates a standard IIoT scenario with three communication layers, each with varying vulnerabilities and security needs: **Not important**, **Important**, and **Very important**. These classifications guide resource prioritization. Security costs are categorized as **Not expensive**, **Expensive**, and **Very expensive**, where **Very expensive** signifies higher costs and advanced security measures for more sophisticated threats. This classification helps optimize the balance between security and budget, enabling the algorithm to manage trade-offs effectively. Table II details the cybersecurity needs and costs for each communication layer.

TABLE II
CYBERSECURITY AND COST CHARACTERISTICS OF THE THREE COMMUNICATION LAYERS FOR THE CONSIDERED IIOT SYSTEM

Layer	**Cybersecurity Features**		
	Confidentiality	**Integrity**	**Availability**
Access Layer	Not important, Not expensive	Very important, Expensive	Important, Not expensive
Network Layer	Very important, Very expensive	Very important, Not expensive	Not important, Not expensive
Application Layer	Not important, Not expensive	Important, Expensive	Important, Very expensive

Legend: Numerical values (3, 2, 1) represent priority for security/expected cost levels: 3 = very important/very expensive, 2 = important/expensive, 1 = less important/less expensive.

The attributes in Table II are assigned numerical values for analysis, as indicated in the table's legend. This numerical scaling, used in techniques like Analytic Hierarchy Process (AHP) and Fuzzy Logic, facilitates structuring and prioritizing decision criteria, enabling systematic comparison and integration into mathematical models. It leads to the creation of matrices M_{SV} and M_{CV}, which are essential for optimization algorithms. Prioritizing higher values ensures effective resource allocation and enhances decision-making by capturing real-worldIIoT complexities.

In the current study, experiments were designed using simulated data to reflect typical IIoT environments, including diverse security requirements and cost structures. These simulations focused on evaluating the methodology's performance across synthetic scenarios, which allowed flexibility in testing key parameters under controlled conditions. While no specific external dataset was utilized, the results demonstrate the theoretical applicability and robustness of the proposed optimization framework.

The values assigned to the matrices M_{SV} and M_{CV} in equations (5) and (6) are derived based on the qualitative classifications of the layers' security and cost attributes. Each value corresponds to the importance or expense of securing a specific layer, as defined in Table II. The values for M_{SV} represent the security needs (Confidentiality, Integrity, and Availability) of each layer, with higher values indicating more critical security requirements. Similarly, the values for M_{CV} reflect the cost constraints, where higher values correspond to more expensive security measures. These matrices are then used in the optimization process to balance security requirements and cost constraints. Therefore, the values are not arbitrary but reflect the practical and strategic priorities for cybersecurity investments IIoT scenario.

$$M_{SV} = \begin{bmatrix} 1 & 3 & 2 \\ 3 & 3 & 1 \\ 1 & 2 & 2 \end{bmatrix} \tag{5}$$

$$M_{CV} = \begin{bmatrix} 1 & 2 & 2 \\ 3 & 1 & 1 \\ 1 & 2 & 2 \end{bmatrix} \tag{6}$$

In solving the optimization problem, two critical constraints are essential: the minimum security level $\underline{S_i}$ and the maximum budget $\overline{C_i}$ for each communication layer. These constraints balance security needs with financial limits, ensuring feasible solutions. Widely used in operations research and project management, these constraints optimize resource allocation while maintaining service levels or project schedules. In our approach, the constraints $\underline{S_i}$ and $\overline{C_i}$ are derived from the matrices M_{SV} and M_{CV}. The security constraint $\underline{S_i}$ is based on the highest security value in the corresponding row of M_{SV}, ensuring adequate protection. The budget constraint $\overline{C_i}$ is the sum of all cost values for each layer in M_{CV}, ensuring financial limits are respected. These constraints, as summarized in Table III, ensure that each communication layer is secured based on its risk profile and budget.

TABLE III
THE VALUES ASSIGNED FOR THE CONSTRAINTS $\underline{S_i}$ AND $\overline{C_i}$

Layer	**Constraints**	
	$\underline{\mathbf{S}_i}$	$\overline{C_i}$
Access Layer	3	5
Network Layer	3	5
Application Layer	2	5

To address the optimization problem, we utilized the iterative method [26] [27] for precise optimization through mixed-integer linear programming (MILP) and the NSGA-II genetic algorithm [26] [28] for handling multi-objective trade-offs. The iterative method provides exact solutions crucial for cybersecurity resource allocation, while NSGA-II effectively navigates complex trade-offs in IIoT scenarios [29] [30]. These complementary approaches ensure rigorous and adaptable optimization of IIoT security.

To evaluate the iterative and NSGA-II genetic methods, we tested ten randomly generated instances (I_1 to I_{10}) to assess performance under varied scenarios. We fixed the security level upper limit $\overline{S_i} = 10$ and the budget lower limit $\underline{C_i} = 1$ to standardize testing and focus on realistic constraints. Each instance underwent 100 independent tests to ensure robust and reliable results, reflecting best practices in optimization as noted by [31], [32], and [33]. For NSGA-II, we used a population size of $n = 200$, 1000 generations, a crossover probability of 0.9, and a mutation probability of 0.4 to balance exploration and exploitation, aligning with established evolutionary computation practices [29], [31], [32], and [33].

B. Obtained results with iterative method

Table IV presents the results of solving the cybersecurity investment problem across various instances using the iterative method, focusing on the IIoT scenario. Each instance evaluates three key layers—Access (ACC), Network (NET), and Application (APP)—in terms of the three critical security features: Confidentiality (Cf_i), Integrity (If_i), and Availability (Af_i). For each layer and feature, the table provides the achieved security level (S) and the corresponding cost (C). The best results in each row are highlighted in **bold** to emphasize the most effective security-cost trade-offs.

TABLE IV
THE ACHIEVED SECURITY LEVEL (S) AND COST (C) WITH ITERATIVE METHOD FOR EACH SECURITY FEATURE (CONFIDENTIALITY, INTEGRITY, AVAILABILITY) ACROSS DIFFERENT INSTANCES AND LAYERS.

Instances	Cf_i (S, C)	If_i (S, C)	Af_i (S, C)
ACC_{I1}	**3.20, 1.40**	4.15, 2.33	4.62, 2.46
NET_{I1}	1.40, 3.89	**5.30, 1.58**	**8.23, 1.09**
APP_{I1}	**7.60, 0.95**	8.53, 2.23	2.72, 2.75
ACC_{I2}	2.90, 1.93	**6.83, 1.00**	4.12, 1.72
NET_{I2}	**7.40, 0.70**	6.70, 2.07	1.57, 1.34
APP_{I2}	1.70, 2.18	4.69, 2.49	**5.05, 4.50**
ACC_{I3}	2.43, 0.47	**8.97, 2.25**	4.78, 2.06
NET_{I3}	**8.47, 2.60**	8.02, 1.07	1.28, 1.22
APP_{I3}	2.30, 0.72	**6.66, 1.94**	4.52, 2.11
ACC_{I4}	6.70, 0.80	**7.89, 2.26**	1.23, 2.15
NET_{I4}	**6.92, 2.32**	1.40, 4.00	1.79, 3.08
APP_{I4}	5.81, 1.50	**8.93, 2.73**	8.01, 2.00
ACC_{I5}	1.61, 0.00	6.01, 1.37	**8.89, 3.32**
NET_{I5}	**6.83, 1.35**	5.71, 0.67	6.39, 1.06
APP_{I5}	2.60, 1.05	4.84, 2.90	4.52, 5.65
ACC_{I6}	**8.05, 2.20**	3.06, 3.13	7.60, 2.51
NET_{I6}	4.52, 4.50	**7.93, 1.54**	3.84, 2.21
APP_{I6}	1.85, 1.01	5.81, 2.99	3.51, 3.19
ACC_{I7}	1.46, 0.00	6.30, 1.70	3.57, 2.51
NET_{I7}	**7.04, 2.66**	6.13, 1.10	2.25, 2.26
APP_{I7}	2.78, 4.87	4.43, 3.26	5.13, 1.70
ACC_{I8}	**7.79, 1.13**	6.51, 2.91	5.10, 2.57
NET_{I8}	**7.50, 3.12**	4.85, 0.46	5.38, 1.05
APP_{I8}	4.65, 1.07	**9.70, 2.69**	1.93, 2.77
ACC_{I9}	3.00, 3.71	3.00, 1.05	3.76, 1.71
NET_{I9}	4.86, 0.00	4.27, 2.00	2.33, 0.50
APP_{I9}	3.64, 2.00	4.65, 1.88	**8.08, 3.50**
ACC_{I10}	2.42, 0.36	**6.86, 2.50**	4.05, 2.44
NET_{I10}	**7.95, 3.52**	6.31, 1.11	2.20, 1.20
APP_{I10}	1.05, 0.19	4.85, 2.77	4.60, 2.45

The results are presented in a tuple format (e.g., (3.20, 1.40) for ACC I1 in Confidentiality and Cost). These tuples represent two values: the **first value** corresponds to the **achieved security level (S)** for the respective feature, and the **second value** refers to the **associated cost (C)** of achieving that level of security. For example, for **ACC I1**, the tuple (3.20, 1.40) means that the achieved security level for Confidentiality is 3.20, and the cost for achieving this level of security is 1.40.

To assess the effectiveness of the proposed approach, we analyzed four key criteria: (i) achieving the targeted security levels for the CIA features, ensuring necessary protection; (ii) staying within the specified budget for each CIA characteristic, ensuring cost-efficiency; (iii) balancing both security and budget requirements simultaneously; and (iv) meeting security and budget constraints while adhering to minimum security limits ($\underline{S_i}$) and maximum cost limits ($\overline{C_i}$), ensuring an optimal and feasible solution. These criteria are essential for validating the practical applicability of our approach in real-world IIoT systems. The percentage of solutions meeting each criterion is shown in Figure 4.

The study reveals significant variability in cybersecurity investment outcomes within IIoT environments, underscoring the necessity for context-specific strategies. The iterative method demonstrates that high security levels can often be achieved cost-effectively by targeting resources at critical layers. Instances such as NET_{I1} and NET_{I10} exemplify how moderate investment levels can yield high security, especially for Confidentiality and Integrity, as shown by the Pareto curves in Figure 3, which illustrate optimal trade-offs.

Figure 4 provides a detailed evaluation of the percentage of solutions meeting specific criteria: targeted security levels for CIA; budget compliance; combined security and budget requirements; and comprehensive adherence to minimum security limits ($\underline{S_i}$) and maximum cost limits ($\overline{C_i}$). Results show that 50% of solutions meet the security level targets, while 40% adhere to the budget, suggesting a generally effective allocation of resources. Notably, only 20% of solutions meet both security and budget criteria, and just 10% achieve complete compliance with all constraints, indicating the need for further refinement of the iterative method to meet the complex demands of real-world IIoT systems.

The presence of instances like NET_{I3} and NET_{I7}, which efficiently balance Integrity, and APP_{I9}, which optimally handles Availability, further supports the value of a tailored investment strategy. These instances illustrate how security improvements in one area may increase costs or reduce efficiency in another. For instance, as shown in NET_{I7}, high Integrity (6.13) is achieved with a relatively low cost (1.10), yet this efficiency is not consistently replicable across all layers. Similarly, ACC_{I6} demonstrates a good balance for Confidentiality (8.05) with a moderate cost (2.20).

The findings indicate that while the iterative approach forms a strong basis, incorporating adaptive techniques like machine learning could improve the model's consistency and efficiency. Tailored investment strategies, aligned with specific IIoT security needs and budget constraints, can optimize both protection and cost management. Ultimately, this research emphasizes the importance of flexible, data-driven approaches to cybersecurity investment, essential for effectively addressing the diverse security requirements of IIoT systems.

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2025.3525779

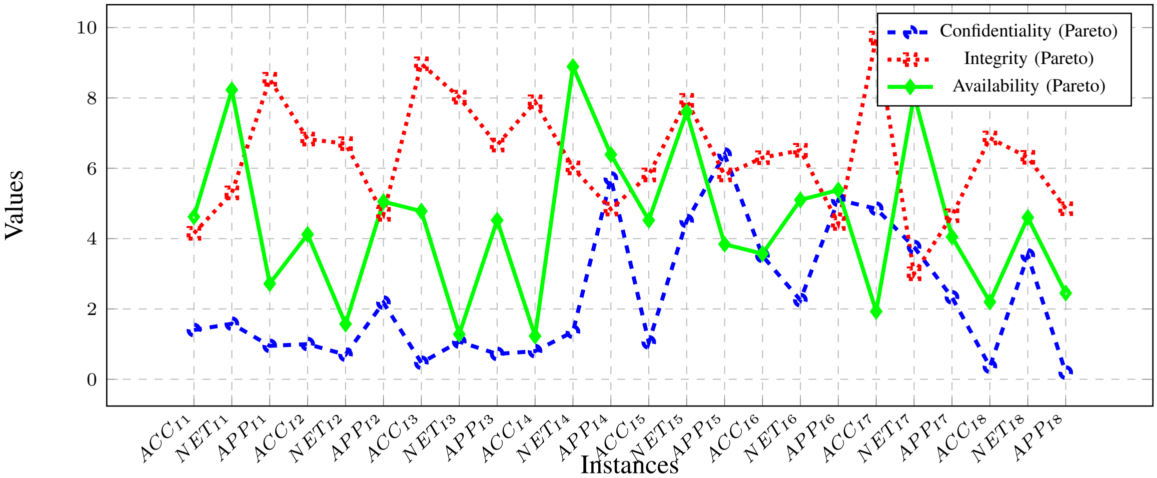

Fig. 3. Pareto Curves Across IIoT Instances (Iterative method)

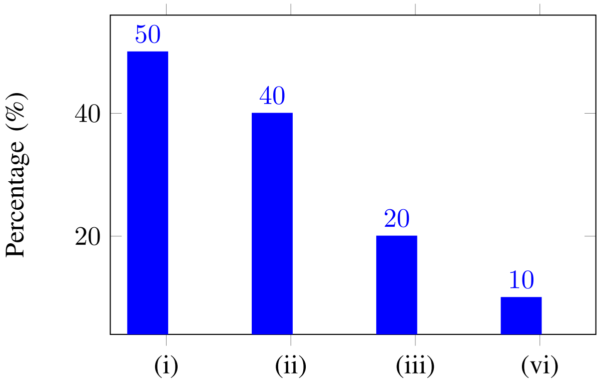

Fig. 4. Effective solution rates with iterative method.

C. Obtained results with genetic method

Our approach to addressing the cybersecurity challenge employs the NSGA-II algorithm, a powerful and efficient genetic algorithm. In this implementation, NSGA-II is configured with a population size of 200 and executed over 1000 generations. The algorithm uses crossover and mutation operators with probabilities of 0.9 and 0.4, respectively. The performance results and outcomes of this genetic approach are represented and detailed in TABLE V. The best results in each row are highlighted in **bold** to emphasize the most effective security-cost trade-offs.

The analysis results reveals that the Genetic Method efficiently balances security levels and costs across various IIoT instances. For instance, the Genetic Method achieved significant improvements in reducing costs while maintaining high security levels compared to the Iterative Method. Specifically, for instance ACC_{I1}, the Genetic Method lowered the confidentiality cost from 1.40 to 0.45, while achieving a comparable security level of 4.04. Similarly, for NET_{I3}, the Genetic Method reduced the cost from 2.60 to 1.60 while maintaining security at 6.07. These examples highlight the Genetic Method's capability to optimize both security and cost effectively, demonstrating its robustness in addressing the cybersecurity investment problem.

TABLE V
OBTAINED RESULTS WITH GENETIC METHOD.

Instances	**IIoT**		
	Cf_i (S, C)	If_i (S, C)	Af_i (S, C)
ACC_{I1}	1.58, 0.45	**6.15, 2.15**	4.04, 2.16
NET_{I1}	**5.81, 2.89**	6.30, 0.88	4.41, 0.19
APP_{I1}	1.20, 0.77	3.93, 2.03	**5.72, 1.81**
ACC_{I2}	3.90, 1.05	4.83, 1.90	**4.77, 2.12**
NET_{I2}	1.66, 3.00	3.55, 0.77	**1.82, 1.24**
APP_{I2}	4.18, 1.16	2.69, 1.79	**6.05, 2.05**
ACC_{I3}	1.80, 1.47	**6.86, 2.05**	2.30, 3.96
NET_{I3}	**6.07, 1.60**	5.72, 3.07	0.28, 2.22
APP_{I3}	1.02, 1.72	4.00, 1.74	**4.39, 2.51**
ACC_{I4}	**5.22, 0.80**	2.22, 1.46	4.06, 2.25
NET_{I4}	2.74, 3.02	**5.86, 1.20**	4.30, 1.08
APP_{I4}	**6.01, 1.26**	3.93, 1.73	1.45, 2.00
ACC_{I5}	1.66, 1.68	**6.94, 2.10**	3.99, 1.32
NET_{I5}	**6.83, 1.55**	5.71, 1.67	1.39, 2.06
APP_{I5}	1.06, 1.15	3.84, 2.45	**4.52, 3.65**
ACC_{I6}	2.05, 3.00	**4.06, 1.13**	2.60, 2.21
NET_{I6}	2.80, 3.50	2.93, 0.54	**5.96, 1.21**
APP_{I6}	**4.85, 1.07**	3.81, 2.52	2.51, 2.19
ACC_{I7}	2.43, 0.79	**7.00, 1.76**	5.07, 2.01
NET_{I7}	**7.35, 2.16**	6.52, 1.10	0.25, 0.26
APP_{I7}	0.78, 0.87	**3.43, 2.16**	3.19, 1.95
ACC_{I8}	0.79, 1.13	**5.51, 2.11**	2.10, 2.57
NET_{I8}	**5.50, 3.17**	5.95, 0.10	1.38, 1.33
APP_{I8}	1.35, 1.07	**3.17, 2.19**	3.93, 1.97
ACC_{I9}	4.00, 2.11	**4.59, 3.05**	5.06, 1.41
NET_{I9}	3.86, 1.00	**5.27, 2.00**	3.80, 1.18
APP_{I9}	3.35, 2.35	3.65, 1.12	**5.08, 2.20**
ACC_{I10}	1.42, 0.66	**6.86, 1.82**	5.05, 2.24
NET_{I10}	**6.00, 2.52**	7.01, 1.11	1.20, 0.80
APP_{I10}	1.05, 0.59	**3.85, 1.97**	1.60, 2.21

Figure 5 illustrates the trade-offs between Confidentiality, Integrity, and Availability using the genetic optimization method. The Pareto curves highlight key insights: instances like NET_{I1} (Confidentiality = 5.81) and APP_{I4} (Confidentiality = 6.01) excel in confidentiality, while APP_{I5} (Integrity = 6.94) and NET_{I3} (Integrity = 5.72) achieve superior integrity scores. Availability varies, with APP_{I2} (Availability = 6.05) and NET_{I6} (Availability = 5.96) offering higher values compared to instances like APP_{I1} (Availability = 5.72). For instance, NET_{I1} also provides a balanced trade-off with a moderate cost (C = 2.89) and relatively high confidentiality. These results demonstrate the balance achieved between objectives, with some instances excelling in specific

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2025.3525779

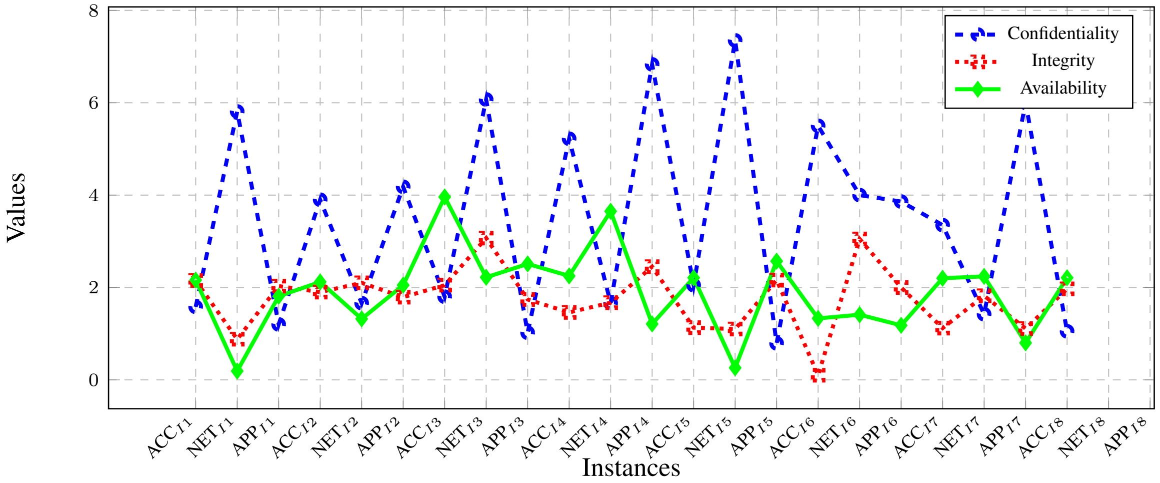

Fig. 5. Pareto Curves Across IIoT Instances (Genetic method)

aspects, while others provide a more balanced trade-off.

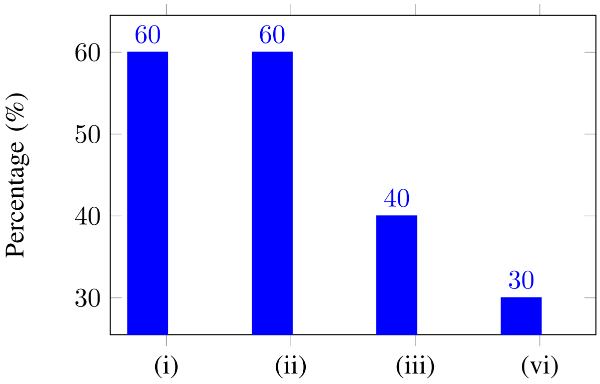

Fig. 6. Effective solutions rates with genetic method.

The results demonstrate the genetic method’s effectiveness in optimizing IIoT security. It successfully addresses key criteria, with 30% of solutions meeting all security and cost requirements. In smart manufacturing, 60% of solutions meet security standards like ISA/IEC 62443, while 60% align with cost constraints. Notably, 20% of solutions show improved balance between security and costs, a critical factor for smart cities. These findings highlight the method’s robust capability to optimize cybersecurity investments in complex IIoT environments.

D. Comparison Between Iterative and Genetic Methods

To assess the effectiveness of the proposed approach, we compared the iterative and genetic methods for solving the cybersecurity investment problem in IIoT environments. As shown in Figure 7, the genetic method consistently outperforms the iterative method across all criteria. Specifically, the genetic method achieves a 60% success rate for both the targeted security levels (Confidentiality, Integrity, and Availability) and budget adherence criteria, compared to 50% and 40% success rates with the iterative method. This reflects the genetic method’s ability to more effectively meet high-priority requirements without exceeding specified cost limits.

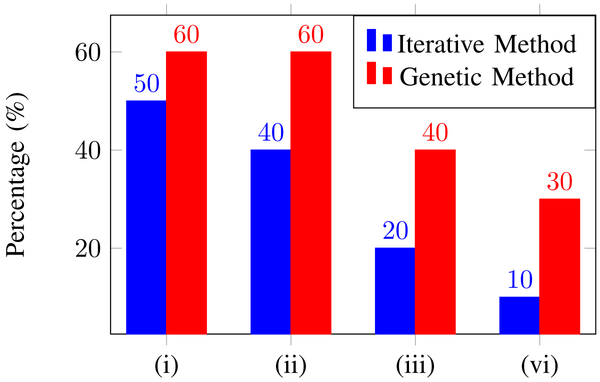

Fig. 7. Comparison between iterative and genetic methods.

Moreover, for balancing security and budget constraints, the genetic method maintains a 40% success rate against the iterative method’s 20%, underscoring its adaptability in handling competing demands. For scenarios where minimum security limits ($\underline{S_i}$) and maximum cost limits ($\overline{C_i}$) must be balanced, the genetic method continues to lead with a 30% success rate compared to only 10% for the iterative method.

These results indicate that the genetic method not only achieves superior performance across all criteria but also proves more reliable and adaptable for complex, real-world IIoT applications. In high-demand environments, such as smart manufacturing systems or expansive smart city infrastructures, this method’s scalability and cost-efficiency make it optimal for balancing stringent security and budgetary requirements, ensuring robust and sustainable cybersecurity solutions.

V. Conclusion and Future Work

This article introduces a bi-objective optimization framework tailored for cybersecurity investment in IIoT environments, aiming to balance robust security with cost management. The framework ensures high levels of confidentiality, integrity, and availability across communication layers, while optimizing security investments within budget constraints. A comparative analysis of iterative and genetic algorithms demonstrates the superior performance of the genetic method. The genetic method outperforms the iterative approach with a 60% success rate in meeting security targets (Confidentiality, Integrity, and Availability) and budget adherence, compared to 50% and 40%, respectively, with the iterative method. Furthermore, the genetic method excels in balancing security and cost constraints with a 40% success rate, against the iterative method's 20%, and leads in handling scenarios where security and cost limits must be balanced, achieving a 30% success rate compared to 10% for the iterative method. These findings highlight the genetic algorithm's ability to explore a broader solution space and provide more adaptable, cost-efficient cybersecurity solutions for IIoT systems. The results underscore its effectiveness in real-world IIoT applications, such as smart manufacturing and smart city infrastructures, where scalability and cost-efficiency are essential for ensuring robust, sustainable cybersecurity.

To advance our approach and meet the evolving needs of IIoT environments, we propose several key research directions. Optimizing model parameters will be vital for accurately representing IIoT system complexities and cybersecurity requirements, while incorporating AI for vulnerability prediction will enhance adaptability to emerging threats, fostering more dynamic security management. Applying the approach to real-world case studies in sectors such as manufacturing, energy, and transportation will validate its practical use and refine its applicability. Benchmarking the framework against established methods using publicly available datasets will demonstrate its effectiveness and ensure alignment with, or improvement over, existing strategies. Expanding simulations to include varied IIoT configurations and attack scenarios will provide a comprehensive assessment of robustness and scalability. Developing a user-friendly interface will facilitate interaction and improve usability for decision-makers, allowing them to visualize optimization results and adjust parameters according to industrial needs. These efforts aim to optimize cybersecurity and help organizations protect critical infrastructure from cyber threats.

References

[1] M. Alabadi, A. Habbal, and X. Wei, *Industrial Internet of Things: Requirements, Architecture, Challenges, and Future Research Directions*, *IEEE Access*, vol. 10, pp. 66374-66400, 2022.

[2] D. G. S. Pivoto, L. F. F. de Almeida, R. da Rosa Righi, J. J. P. C. Rodrigues, A. Baratella Lugli, and A. M. Alberti, *Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review*, *Journal of Manufacturing Systems*, vol. 58, pp. 176-192, 2021.

[3] General Electric, "How GE Uses IIoT to Improve Manufacturing," 2019. [Online]. Available: https://www.ge.com/digital/iiot-manufacturing.

[4] Siemens, "Siemens IIoT Solutions for Predictive Maintenance," 2020. [Online]. Available: https://new.siemens.com/global/en/products/services/digital-enterprise/iiot.html.

[5] WannaCry Attack Report, "Analysis of the 2017 WannaCry Ransomware Attack," 2017. [Online]. Available: https://www.cybersecurityreport.com/wannacry-2017.

[6] J. Smith, "Best Practices in Cybersecurity for IIoT Systems," *Cybersecurity Journal*, vol. 15, no. 3, pp. 45-57, 2021.

[7] R. Roman, J. Zhou, and J. Lopez, "On the Features and Challenges of Security and Privacy in Distributed Internet of Things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2011.

[8] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, Privacy, and Trust in Internet of Things: The Road Ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[9] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, Investments, and Challenges for Enterprises," *Business Horizons*, vol. 61, no. 4, pp. 577–590, 2018.

[10] E. Fernandes, A. Rahmati, J. Jung, and A. Prakash, "Security Implications of Permission Models in Smart-Home Application Frameworks," *IEEE Security and Privacy*, vol. 15, no. 2, pp. 60–70, 2016.

[11] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog Computing for the Internet of Things: Security and Privacy Issues," *IEEE Internet Computing*, vol. 21, no. 2, pp. 34–42, 2017.

[12] M. Das, "Two-Factor User Authentication in Wireless Sensor Networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1086–1090, 2009.

[13] I. Wagner and V. R. Ganapathy, "Practical Network Latency Attacks Against Tor Hidden Services," *IEEE Security and Privacy*, vol. 15, no. 4, pp. 29–37, 2017.

[14] K. Tange, A. Mukherjee, and D. Mukhopadhyay, "Lightweight Encryption for IoT: A Comparison of Block Ciphers in Terms of Security and Performance," *Journal of Cryptographic Engineering*, vol. 7, no. 3, pp. 255–268, 2017.

[15] Y. Zhang, N. Chen, W. Luo, and X. Wang, "Anomaly Detection in IoT Systems Using Machine Learning Algorithms," *IEEE Access*, vol. 6, pp. 70772–70782, 2018.

[16] H. Kim, M. Shin, and H. Lee, "Blockchain-Based Secure Firmware Update for Embedded Devices in an IoT Environment," *IEEE Access*, vol. 8, pp. 102360–102371, 2020.

[17] R. Singh, A. Jain, and S. Kumar, "Security and resource constraints in Industrial Internet of Things (IIoT): A comprehensive review," *Journal of Industrial Information Integration*, vol. 19, p. 100162, 2021.

[18] R. S. Dhillon and S. Kapoor, "Resource management and security challenges in IIoT systems: A review of recent trends and solutions," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 4, pp. 2764–2772, 2022.

[19] S. Lalla and A. Kumar, "Bi-objective optimization models for balancing security and resource efficiency in networks," *Computers Electrical Engineering*, vol. 74, pp. 72–84, 2019.

[20] M. Li and X. Wang, "A bi-objective optimization approach for secure and efficient communication in IoT-based industrial environments," *Journal of Network and Computer Applications*, vol. 153, p. 102531, 2020.

[21] Y. Gong, J. Zhou, Q. Wu, M. Zhou, and J. Wen, "A Length-Adaptive Non-Dominated Sorting Genetic Algorithm for Bi-Objective High-Dimensional Feature Selection," *IEEE/CAA Journal of Automatica Sinica*, vol. 10, no. 9, pp. 1834-1844, September 2023.

[22] H. Li, D. Wang, M. Zhou, Y. Fan, and Y. Xia, "Multi-Swarm Co-Evolution Based Hybrid Intelligent Optimization for Bi-Objective Multi-Workflow Scheduling in the Cloud," *IEEE Transactions on Parallel and Distributed Systems*, vol. 33, no. 9, pp. 2183-2197, 1 Sept. 2022.

[23] J. Xu, Y. Zhou, Y. Ding, D. Yang, and L. Xu, "Biobjective Robust Incentive Mechanism Design for Mobile Crowdsensing," *IEEE Internet of Things Journal*, vol. 8, no. 19, pp. 14971-14984, 1 Oct. 2021.

[24] H. Yuan, H. Liu, J. Bi, and M. Zhou, "Revenue and Energy Cost-Optimized Biobjective Task Scheduling for Green Cloud Data Centers," *IEEE Transactions on Automation Science and Engineering*, vol. 18, no. 2, pp. 817-830, April 2021.

[25] K. Stoilova and T. Stoilov, *Business Management by Portfolio Optimization Model*, *2023 XXXII International Scientific Conference Electronics (ET)*, pp. 1-4, 2023.

[26] S. Bokhari, S. Hamrioui, and M. Aider, *Cybersecurity Strategy Under Uncertainties for an IoE Environment*, *Journal of Network and Computer Applications*, vol. 205, article 103426, 2022.

[27] D. A. Kakkad, I. E. Grossmann, B. Springub, C. S. Galbraith, and M. A. Lovell, "Optimization of Industrial Control Systems in the Internet of Things Environment," *Applied Computational Intelligence and Soft Computing*, vol. 2019, 2019.

[28] J. McCall, Genetic algorithms for modelling and optimisation, Journal of Computational and Applied Mathematics, 184, 1, pp: 205-222, 2005.

[29] N. Srinivas and K. Deb, "Multiobjective Optimization Using Nondominated Sorting in Genetic Algorithms," *Evolutionary Computation*, vol. 2, no. 3, pp. 221–248, 1994.

[30] N. Koroniotis, N. Moustafa, T. Janicke, B. Turnbull, and M. Hammoudeh, "Towards the Development of Realistic Botnet Dataset in the Internet of Things for Network Forensic Analytics: Bot-IoT Dataset," *Future Generation Computer Systems*, vol. 100, pp. 779–796, 2019.

[31] K. Deb, A. Pratap, S. Agarwal, and T. Meyarivan, "A Fast and Elitist Multiobjective Genetic Algorithm: NSGA-II," *IEEE Transactions on Evolutionary Computation*, vol. 6, no. 2, pp. 182–197, 2002.

[32] D. E. Goldberg, "Genetic Algorithms in Search, Optimization, and Machine Learning," *Addison-Wesley*, 1989, ISBN: 978-0201157673.

[33] Z. Michalewicz, "Genetic Algorithms + Data Structures = Evolution Programs," *Springer*, 1996, ISBN: 978-3540609244.