

Designing robust cybersecurity measures using optimization techniques in enterprise information

Manoj Kumar Srivastava [§]

Department of Computer Science & Engineering

Ajay Kumar Garg Engineering College

Ghaziabad 201015

Uttar Pradesh

India

Vivek Kumar [†]

EXL Service Holding LLC

Jersey City

New Jersey 07302

United States

Lalit Agrawal ^{*}

School of Computer Science and Engineering

Ramdeobaba University

Nagpur 440013

Maharashtra

India

I. M. Christina Febiula [‡]

School of Management

S.A. College of Arts & Science

Chennai 600077

Tamil Nadu

India

[§] E-mail: srivastava.mk79@gmail.com

[†] E-mail: valueadmire@gmail.com

^{*} E-mail: agrawalls@rknec.edu (Corresponding Author)

[‡] E-mail: christinafebiulaim@sacas.ac.in

Asha Abraham Chandi [@]
Om Retail Oil Inc.
Pittsburgh
Pennsylvania 15112
U.S.A.

Nishith Singh [#]
Department of BFSI - Research and Development
Xoriant India Pvt. Ltd.
Gurugram 122009
Haryana
India

Abstract

Businesses are facing new online dangers because their IT systems are getting more complicated. To protect themselves, they need strong, flexible, and resource-efficient defences. This paper looks at how optimization methods can be used to make business security systems stronger. Linear and nonlinear optimization models help you make structured decisions that minimize costs and risks, and metaheuristic techniques like genetic algorithms, particle swarm optimization, and ant colony optimization let you deal with threats in a way that adapts to them. It is possible to combine goal functions and limits that show how information flows in a business using maths. The results show that methods based on optimization improve the reliability, efficiency, and flexibility of defending sensitive business information assets.

Subject Classification: 46N10, 13P25.

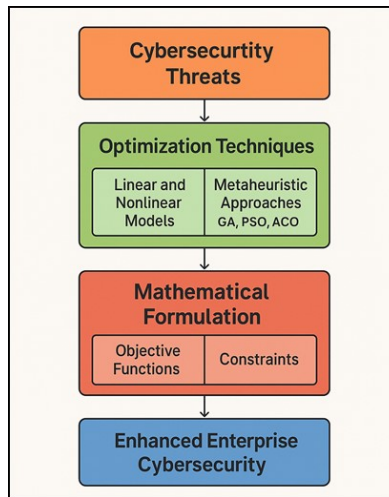
Keywords: Cybersecurity, Optimization, Enterprise information, Metaheuristics, Risk management.

I. Introduction

Organizations are more vulnerable to new and changing cybersecurity risks because they depend more and more on corporate information systems. Ransomware, hacking, insider threats, and distributed denial-of-service (DDoS) operations are all complex attack routes that put the privacy, security, and availability of important data at risk [1, 2]. Even though traditional security methods are necessary, they don't always work well in today's large and complex business settings. Because of this, businesses are looking for methodical and scientifically sound ways to improve resilience while also making sure that resources are used efficiently [3, 4]. Figure 1 illustrates optimization-based methods enhancing enterprise cybersecurity resilience [5]. Optimization methods have become useful for dealing with these issues because they provide models that balance security goals with practical limitations [6].

[@] E-mail: asha.chandi6@gmail.com

[#] E-mail: nishith.creativearchitect@gmail.com

**Figure 1****Optimization-Driven Framework for Enhancing Enterprise Cybersecurity**

It is possible to make decision-making models for risk assessment, anomaly spotting, and access control using both linear and nonlinear optimization methods [7, 8]. In the same way, metaheuristic methods like genetic algorithms, particle swarm optimization, and ant colony optimization make it possible to study a lot of different ways to stop changing threats [9]. By combining optimization with cybersecurity, companies can create defence plans that are flexible, scalable, and cost-effective, which improves their total information security [10, 11].

II. Optimization Techniques in Cybersecurity*A. Linear and nonlinear optimization models*

Linear and nonlinear optimization models employ math to help make defensive decisions that use resources wisely, keep risks to a minimum, and balance cost, performance, and resilience [12, 13].

Nonlinear risk relationship:

$$R(x) = \sum (a_i * x_i^2) \quad (1)$$

Objective changes to:

$$\text{Minimize } Z = \sum (c_i * x_i + a_i * x_i^2) \quad (2)$$

Security effectiveness constraint:

$$\sum (e_i * x_i) \geq E_{min}.$$

Complete nonlinear formulation:

Minimize

$$Z = \sum c_i * x_i + \sum a_i * x_i^2 + \sum \beta_{ij} * x_i * x_j \quad (3)$$

Under business limits, the best allocation x^* lowers cyber risk to the lowest level.

B. Metaheuristic approaches

Metaheuristic methods like Genetic Algorithms, Particle Swarm Optimization, and Ant Colony Optimization are strong ways to improve defence. They are good at solving complicated, nonlinear, and multi-objective problems. This lets resources be allocated more adaptably, intrusion detection get better, latency get lower, and business environments become more resistant to new cyber threats.

Theorem (Metaheuristic-Based Optimization for Robust Cybersecurity in Enterprises): Flow, bandwidth, security, privacy, availability, redundancy, and budget are some of the cybersecurity limitations that can be worked with).

Consider an objective function $F(x)$ where $x = (x_1, x_2, \dots, x_n)$ represents enterprise resource allocations.

Metaheuristic algorithms guarantee probabilistic convergence to near-optimal solutions if $F(x)$ is non-convex and has more than one goal within Ω .

Proof:

Step 1: Problem Formulation

Minimize:

$$F(x) = \alpha_1 * R(x) + \alpha_2 * L(x) - \alpha_3 * S(x) \quad (4)$$

where $R(x)$ = risk cost, $L(x)$ = latency, $S(x)$ = security strength.

Step 2: Metaheuristic Representation

Each candidate solution x^k is a vector of allocations.

- GA encodes x^k as a chromosome; mutation/crossover explore space.
- PSO updates via:

$$v_i^{t+1} = \omega v_i^t + c_1 r_1 (p_i - x_i^t) + c_2 r_2 (g - x_i^t) \quad (5)$$

$$x_i^{t+1} = x_i^t + v_i^{t+1} \quad (6)$$

Step 3. Constraint Handling

Feasible solutions must satisfy:

$$\Sigma (s_i * x_i) \geq S_{min}$$

$$\Sigma (a_i * x_i) \geq A_{min}$$

$$\Sigma (c_i * x_i) \geq C_{min} \quad (7)$$

Infeasible candidates penalized:

$$F'(x) = F(x) + \lambda * P(x) \quad (8)$$

Step 4. Convergence Justification

For iterations $T \rightarrow \infty$:

$$\Pr(F(x^*) - F(x^T) \leq \varepsilon) \rightarrow 1 \quad (9)$$

where x^* = global optimum.

III. Mathematical Formulation

A. Objective functions for cybersecurity data

To improve cybersecurity, the created objective function combines minimizing risk, cutting costs, and increasing efficiency. It makes sure that allocation strategies are strong, efficient, and scalable by balancing weighted risks, resource costs, and logarithmic efficiency gains. This makes sure that enterprises are more resistant to threats and that resources are used most effectively in complex security environments.

Minimize overall risk exposure.

$$\text{Minimize } Z = \sum (w_i * R_i) \quad (10)$$

Express R_i as function of resource x_i :

$$R_i = \frac{a_i}{(1 + b_i * x_i)}. \quad (11)$$

Substitute into objective:

$$Z = \sum \left(w_i * \frac{a_i}{(1 + b_i * x_i)} \right). \quad (12)$$

Consider cost function:

$$C = \sum (c_i * x_i). \quad (13)$$

Multi-objective function:

$$\text{Minimize } F = \lambda_1 * Z + \lambda_2 * C. \quad (14)$$

Add effectiveness function:

$$E = \sum (e_i * \log(1 + x_i)). \quad (15)$$

Adjusted objective:

$$\text{Minimize } F = \lambda_1 * Z + \lambda_2 * C - \lambda_3 * E. \quad (16)$$

Expand to full expression:

$$F = \sum \left(\lambda_1 * w_i * \frac{a_i}{(1 + b_i * x_i)} \right) + \sum (\lambda_2 * c_i * x_i) - \sum (\lambda_3 * e_i * \log(1 + x_i)). \quad (17)$$

Result: Objective function tailored for cybersecurity metrics.

B. Constraints based on enterprise information flow

This theorem makes sure that it is possible and that the best cybersecurity resources are allocated so that business information flows while keeping integrity, privacy, availability, redundancy, and efficiency.

Theorem: Let x_i = resources allocated to node i in an enterprise network, with flow variables f_{ij} representing data transfer between nodes.

Define the feasible region

$$\Omega = \{ (x_i, f_{ij}) \mid \text{satisfying constraints (18)–(global budget)} \}.$$

Then:

1. $\Omega \neq \emptyset$ (non-empty feasible region exists) if budget and integrity allocations are consistent.
2. Any optimization problem of the form

Minimize $F(x, f)$ subject to $(x_i, f_{ij}) \in \Omega$ is guaranteed to have at least one solution

Proof:

Step 1. Flow conservation

$$\sum f_{ji} \geq \sum f_{ij}, \forall i$$

Ensures no node transmits more data than it receives.

Step 2. Bandwidth feasibility

$$\sum f_{ij} \leq B_i, \forall i$$

Feasible since $B_i > 0$ and $f_{ij} = 0$ is valid.

Step 3. Security threshold

$$\sum (s_i * x_i) \geq S_{min}$$

If some $s_i > 0$, feasible allocations exist

Step 4. Integrity requirement

$$x_i \geq l_i, \forall i$$

Feasibility requires $\sum l_i \leq B$.

Step 5. Dependency constraint

$$x_j \leq d_{ij} * x_i$$

Linear relation preserves convexity.

Step 6. Latency constraint

$$\sum (l_{ij} * f_{ij}) \leq L_{max}$$

Feasible since $f_{ij} = 0$ is possible.

Step 7. Confidentiality, availability, redundancy

$$\sum (c_i * x_i) \geq C_{min}$$

$$\sum (a_i * x_i) \geq A_{min}$$

$$x_i + x_j \geq R_{ij}$$

All linear, convex

IV. Result Discussion

Table 1 shows how well different optimization methods work in cybersecurity. Both linear and nonlinear optimization methods can spot things fairly well, but they use more resources and take longer to respond.

Table 1
Performance of Optimization Models in Cybersecurity

Model / Framework	Detection Accuracy (%)	Resource Utilization (%)	Response Time (ms)
Linear Optimization	88.4	74.2	120
Nonlinear Optimization	90.7	71.6	135
Genetic Algorithm (GA)	92.5	68.3	110
Particle Swarm (PSO)	93.8	66.5	105

Metaheuristic methods work better than standard models. For example, the Genetic Algorithm is more accurate and uses fewer resources.

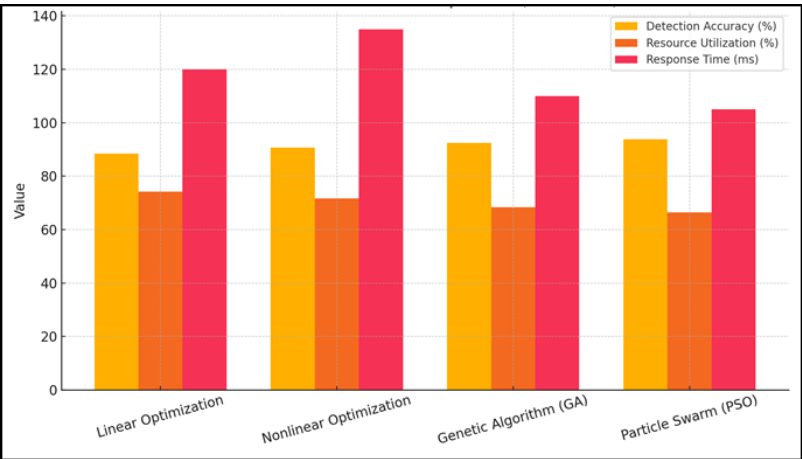


Figure 2
Comparative Analysis of Optimization Models by Accuracy, Efficiency, and Response Time

The best performance comes from Particle Swarm Optimization, which has a high discovery rate (93.8%), good resource utilization (66.5%), and a faster reaction time (105 ms) (shows in figure 2). This makes it perfect for flexible, large-scale business protection settings.

V. Conclusion

This study shows how important optimization methods are for making business protection stronger. Companies can effectively use their resources, reduce risks, and respond to changing threats by using linear, nonlinear, and metaheuristic models. Frameworks that are driven by optimization make sure that defence is preventative while keeping cost and speed in mind. When these methods are combined, businesses can make security systems that are strong, flexible, and smart. This protects private data and builds trust in their IT systems as online threats change.

References

- [1] K. Sathupadi, "A hybrid deep learning framework combining on-device and cloud-based processing for cybersecurity in mobile cloud environments," *Int. J. Inf. Cybersecur.*, vol. 7, pp. 61–80 (2023).
- [2] S. M. Zohaib, S. M. Sajjad, Z. Iqbal, M. Yousaf, M. Haseeb, and Z. Muhammad, "Zero Trust VPN (ZT-VPN): A Systematic Literature Review and Cybersecurity Framework for Hybrid and Remote Work," *Information*, vol. 15, pp. 734 (2024).
- [3] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture. Gaithersburg, MD, USA: National Institute of Standards and Technology (2020).
- [4] R. Chandramouli, Guide to a Secure Enterprise Network Landscape. Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology (2022).
- [5] S. S. Wang and U. Franke, "Enterprise IT service downtime cost and risk transfer in a supply chain," *Oper. Manag. Res.*, vol. 13, pp. 94–108 (2020).
- [6] M. R. Mollahoseini Ardakani, S. M. Hashemi, and M. Razzazi, "A cloud-based solution/reference architecture for establishing collaborative networked organizations," *J. Intell. Manuf.*, vol. 30, pp. 2273–2289 (2019).
- [7] D. Jia and Z. Wu, "Enterprise collaborative integrated management system based on IoT cloud technology," *Mob. Inf. Syst.*, vol. 2022, Article ID 6098201 (2022).
- [8] F. Li and G. Xu, "AI-driven customer relationship management for sustainable enterprise performance," *Sustain. Energy Technol. Assess.*, vol. 52, pp. 102103 (2022).
- [9] A. Papaioannou, A. Dimara, C. S. Kouzinopoulos, S. Krinidis, C. N. Anagnostopoulos, D. Ioannidis, and D. Tzovaras, "LP-OPTIMA: A framework for prescriptive maintenance and optimization of IoT resources for low-power embedded systems," *Sensors*, vol. 24, pp. 2125 (2024).
- [10] A. Dimara, V. G. Vasilopoulos, A. Papaioannou, S. Angelis, K. Kotis, C. N. Anagnostopoulos, S. Krinidis, D. Ioannidis, and D. Tzovaras, "Self-healing of semantically interoperable smart and prescriptive edge devices in IoT," *Appl. Sci.*, vol. 12, pp. 11650 (2022).

- [11] N. N. H. Adenan, A. Nitaj, M. R. K. Ariffin, and N. A. Abu, "Cryptanalysis of a cubic Pell variant of RSA with primes sharing least significant bits," *J. Inf. Optim. Sci.*, vol. 45, no. 5, pp. 1263–1280 (2024).
- [12] S. Saxena, M. Z. Khan, and R. Singh, "Green computing: An era of energy saving computing of cloud resources," *Int. J. Math. Sci. Comput.*, vol. 7, pp. 42–48 (2021).
- [13] W. N. Anandpwar, S. M. Barhate, and M. P. Dhore, "Designing an efficient machine learning-based intrusion detection system for enhanced cyber security in modern networks," *Int. J. Adv. Comput. Theory Eng.*, vol. 14, no. 1, pp. 70–75 (Apr. 2025).

Received May, 2025