EasyChair Preprint

№ 15079

# Mathematical Models and Formulas for AI in Cybersecurity: a Hybrid Cloud Approach

Lincoln Whitelegge



September 26, 2024

# Mathematical Models and Formulas for AI in Cybersecurity: A Hybrid Cloud Approach

Lincoln Whitelegge
*Research Software Engineer*
Tindarey NSW, Australia

***Abstract*—The adoption of hybrid cloud environments introduces new security challenges that can be efficiently addressed using AI-driven solutions. To maximize the effectiveness of these AI systems, mathematical models and algorithms play a critical role in enhancing security measures, detecting threats, and optimizing system performance. This article explores the mathematical foundations behind AI algorithms in cybersecurity, focusing on their application to hybrid cloud infrastructures. Key models such as supervised learning, anomaly detection, encryption schemes, and optimization algorithms will be discussed to illustrate how mathematical formulations ensure robust cloud security.**

***Keywords—Cryptography, Resource Optimization, Linear Programming, Convex Optimization, Game Theory, Nash Equilibrium, RSA Encryption***

## I. Introduction

In cybersecurity, Artificial Intelligence (AI) leverages mathematical models to automate threat detection, classification, and response. The hybrid cloud, a combination of public and private cloud environments, requires sophisticated algorithms to manage its dynamic and distributed nature. By using AI, security systems can process large volumes of data, identify patterns, and predict vulnerabilities with increased precision. This paper presents key mathematical formulas used in AI algorithms for hybrid cloud security, demonstrating their effectiveness in improving cyber defenses.

## II. Mathematical Models in AI for Cybersecurity

AI in cybersecurity operates on fundamental mathematical models that allow machines to learn, classify, and predict threats based on large datasets. These models are powered by several key formulas and techniques, including linear algebra, probability theory, and optimization

### *A. Supervised Learning for Threat Detection*

Supervised learning models are widely used in cybersecurity for threat detection, classification, and anomaly recognition. The primary goal is to classify incoming data points into predefined categories (e.g., safe or malicious traffic) using labeled datasets. A mathematical formulation for supervised learning involves the minimization of a cost function J(θ)J(\theta)J(θ), which measures the difference between predicted and actual outcomes

- Cost Function:

$$J(\theta) = \frac{1}{m}\sum_{i=1}^{m}\left(h_\theta(x^{(i)}) - y^{(i)}\right)^2 \tag{1}$$

Where:

- $h\theta(x(i))$ is the hypothesis (or predicted output) for input *x(i).*
- $y(i)$ is the actual label for the input.
- $m$ is the number of data points.
- $\theta$ represents the model parameters.

This cost function is minimized using gradient descent, a widely used optimization algorithm.

$$\theta_j := \theta_j - \alpha\frac{\partial}{\partial\theta_j}J(\theta) \tag{2}$$

Data points with low probabilities under the Gaussian distribution are flagged as anomalies. These flagged points may indicate potential security threats within the hybrid cloud infrastructure.

## III. Anomaly Detection Using Unsupervised Learning

In hybrid cloud environments, it is often necessary to detect unusual behaviors that may signify security breaches. Unsupervised learning techniques like anomaly detection help in identifying deviations from normal patterns by computing probabilities of data points being part of a known distribution.

For anomaly detection, we assume the data follows a Gaussian (normal) distribution. The formula for the probability density function of a Gaussian distribution is:

$$p(x;\mu,\sigma^2) = \frac{1}{\sqrt{2\pi\sigma^2}}e^{-\frac{(x-\mu)^2}{2\sigma^2}} \tag{3}$$

## IV. Encryption and Cryptography in Hybrid Cloud Security

Encryption plays a vital role in hybrid cloud environments to ensure secure communication, data transmission, and storage. AI models optimize encryption processes to enhance data integrity and confidentiality, but the underlying mathematical principles of cryptography are crucial for cloud security.

Symmetric key encryption, specifically the Advanced Encryption Standard (AES), is one of the most commonly used methods for encrypting data in hybrid cloud systems. AES operates through multiple rounds of cryptographic transformations, such as Sub Bytes, a non-linear substitution process based on a pre-calculated lookup table; Shift Rows, a transposition step where rows of data are shifted by a specific number of bytes; and Mix Columns, a linear transformation over the Galois Field GF(28)GF(2^8)GF(28) that mixes data within columns. These transformations ensure the data remains secure through bit-level encryption. The Add Round Key operation, a bitwise XOR function, applies a round key to the data, ensuring its encryption. These steps are repeated based on the key size, which is usually 128, 192, or 256 bits, with more bits leading to more rounds and greater security.

Public key cryptography, such as the RSA algorithm, is often used in hybrid cloud security to secure data communications between different cloud environments. The RSA algorithm is based on the difficulty of factoring large prime numbers, ensuring strong encryption.

## V. Optimization Algorithms in Cloud Resource Allocation

Optimization algorithms are essential for efficiently allocating resources in hybrid cloud environments, balancing security and performance demands. In cloud security, AI models often rely on optimization techniques to ensure that computational resources are used efficiently while maintaining robust security protocols.

Linear programming is one of the key mathematical methods used to optimize resource allocation in cloud systems. It formulates resource allocation as a minimization problem, aiming to reduce costs such as latency, energy usage, or operational inefficiency. Linear programming is represented through a set of linear inequalities, where constraints like security policies, resource availability, and operational limits are expressed in a matrix format. Cloud service providers use linear programming to manage the allocation of resources such as bandwidth, storage, or computing power, ensuring an optimal balance between performance and security.

Convex optimization is another widely used technique in cloud security management, particularly in configuring firewalls, load balancers, and intrusion detection systems. The convex nature of these problems ensures that any local minimum found is also the global minimum, which simplifies the process of finding optimal security configurations. A typical convex optimization problem involves minimizing an objective function subject to a set of constraints, which represent the system's limitations or security requirements. For example, the objective function might represent the risk of a security breach, while the constraints ensure that the system's resources are not over-allocated. By solving convex optimization problems, administrators can ensure that resources are allocated in a way that minimizes security risks while optimizing cloud performance

## VI. Game Theory in Hybrid Cloud Security

As Game theory offers a mathematical framework for analyzing strategic interactions between different actors in a hybrid cloud environment, particularly between attackers and defenders. By modeling these interactions as a game, cybersecurity professionals can anticipate potential attacks and devise optimal defense strategies.

One of the key concepts in game theory is the Nash Equilibrium, which occurs when neither player has an incentive to change their strategy given the strategy of the opposing player. In the context of cybersecurity, reaching a Nash Equilibrium implies that the defender has optimized their security defenses to the point where any deviation by the attacker would not be beneficial. This means that both the attacker and the defender are playing their best possible strategies against each other.

Mathematically, the Nash Equilibrium is expressed by the condition $ui(si*, s-i*) \geq ui(si, s-i*)$ , where $ui$ represents the utility or payoff of player $i, si*$ is the optimal strategy for player $i, s*-i$ is the optimal strategy of the opposing player. In a hybrid cloud environment, this could mean that a security system is configured in such a way that even if an attacker changes their tactics, they cannot gain an advantage because the defense mechanisms are already in place to mitigate that risk.

By applying game theory, AI-driven security systems can simulate and analyze various attack scenarios, helping organizations to preemptively adjust their defenses. This approach not only enhances security but also helps in resource management by ensuring that defensive measures are focused on the most likely and impactful threats

## Conclusion

Mathematics is at the heart of AI-driven cybersecurity solutions for hybrid cloud environments. The use of supervised learning, anomaly detection, cryptography, optimization algorithms, and game theory equips AI models with the necessary tools to secure dynamic and complex cloud infrastructures. By applying these mathematical models, organizations can better manage threats, enhance resource allocation, and ensure robust security across their hybrid cloud systems

## References


[1] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press

[2] Boyd, S., & Vandenberghe, L. (2004). *Convex Optimization*. Cambridge University Press

[3] Bhadani, U., 2020. Hybrid Cloud: The New Generation of Indian Education Society.

[4] Nesterov, Y. (2004). *Introductory Lectures on Convex Optimization: A Basic Course*. Kluwer Academic Publishers.

[5] Bhadani, U., A Detailed Survey of Radio Frequency Identification (RFID) Technology: Current Trends and Future Directions.

[6] Emanuel, E.J. and Wachter, R.M., 2019. Artificial intelligence in health care: will the value match the hype?. *Jama*, *321*(23), pp.2281-2282..

[7] Bhadani, U., 2022. Comprehensive Survey of Threats, Cyberattacks, and Enhanced Countermeasures in RFID Technology. *International Journal of Innovative Research in Science, Engineering and Technology*, *11*(2).

[8] Lee, Y.C., Wang, C., Zomaya, A.Y. and Zhou, B.B., 2010, May. Profit-driven service request scheduling in clouds. In *2010 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing* (pp. 15-24). IEEE.