

Game-theoretic analysis of healthcare data protection framework

Shekhar M. Kumbhar [§]

Department of Community Medicine

Krishna Institute of Medical Sciences

Krishna Vishwa Vidyapeeth (Deemed to be University)

Karad 415539

Maharashtra

India

Varun Kumar Sharma [†]

Department of Biotechnology and Microbiology

Noida International University

Greater Noida 201312

Uttar Pradesh

India

Sulabha Narendra Patil ^{*}

Department of Engineering Science and Humanities

Vishwakarma Institute of Technology

Pune 411037

Maharashtra

India

D. Anandhi [‡]

Department of Biochemistry

Meenakshi Ammal Dental College & Hospital

Meenakshi Academy of Higher Education & Research

Chennai 600095

Tamil Nadu

India

[§] E-mail: drshekharwinofitlifestyle@gmail.com

[†] E-mail: varun1.sharma@niu.edu.in

^{*} E-mail: sulbha.patil@vit.edu (Corresponding Author)

[‡] E-mail: anandhid@maher.ac.in

P. Ramya Krishna [@]

*Department of Electronics & Communication Engineering
Pragati Engineering College
Kakinada 533437
Andhra Pradesh
India*

Abhishek Dixit [#]

*Department of Computer Science and Engineering (Artificial Intelligence & Machine Learning)
Vardhaman College of Engineering
Shamshabad
Hyderabad 501218
Telangana
India*

Abstract

Strategic attackers, insider and privacy–utility conflicts pose persisting problems to healthcare data protection frameworks. In this study we envision a Game-Theoretic Healthcare Data Protection Model (GHDPM) to make optimal defensive decisions in dynamic cyber-risk scenarios. The methodology models the interactions between the healthcare defenders and attackers as a non-cooperative Stackelberg security game where attacks, expected utility, privacy loss and defense costs are modeled. The best protection strategies are chosen using the concepts of nash equilibrium and payoff optimization. Analysis shows that an equilibrium-based defense strategy will decrease the probability of successful attack by 31.8%, the expected privacy loss by 27.4% with respect to static strategies while at the same time increasing security utility by 22.6%. The essence of the novelty is that adaptive strategic defense modeling takes place. The framework provides quantitative support for decision making in healthcare cybersecurity, showcasing the ability of game theoretic optimization to achieve resilient data protection of healthcare systems that is cost-effective and private.

Subject Classification: 91A16.

Keywords: Healthcare cybersecurity, Game theory, Stackelberg security game, Nash equilibrium, Privacy preservation, Adaptive defense optimization.

1. Introduction

The healthcare sector has been rapidly digitizing workflows, EHRs and all medical devices are interconnected, making healthcare a high-value target for cyber adversaries, and the battle between data utility and data protection is a major governance issue for healthcare systems today [1]. Today, multi-stakeholder collaboration among healthcare providers, regulators, and technology vendors is becoming a key enabler for health big-data ecosystems,

[@] E-mail: pramyakrishna@outlook.com

[#] E-mail: abhishek1554@vardhaman.org

with the value derived from accessing each other's clinical data closely tied to the governance frameworks that allow or prevent knowledge sharing and its reuse. This is further complicated by mobile health platforms as the constant sensor streams and behaviors of patients bring new challenges when it comes to privacy risks that can only be partially foreseen using traditional access-control policies [2]. The use of game-theoretic analysis has been established, as shown by the success of evolutionary and knowledge-synthesis studies, which span strategic behavior across a wide range of healthcare settings, covering strategic actions of patients, providers and adversaries [3]. In the e-health applications, privacy preservation has been regarded as a repeated strategic game in which the decisions of disclosure are made and evolve across rounds as the defenders and adversaries adjust their actions over rounds [4]. Similarly, disclosures in online health communities depend on a user's strategic choice: what benefits will accrue from the disclosure and what risks will arise from non-disclosure [5].

Despite this body of work, the vast majority of healthcare protection frameworks continue to be based on a fixed set of rules, compliance checklists, or access-control matrices—none of which reason about a rational, adaptive adversary—and thereby have no structural protections in place to anticipate the institution-level strategic exploitation of free-riding and under-investment in shared security infrastructure [6, 7]. Where there is uncertainty about the outcomes that are desired and competing goals are explicitly represented, strategic modeling can have a significant impact on the quality of outcomes, as revealed in clinical decision environments that also involve immersive visualization and multi-actor decision support [8, 9]. Fuzzy game-theoretic policy design studies for sustainable health supply chains are also shown to give better performance than the heuristic policy rules when uncertainty is present, and this holds true for other sub-domains of health systems such as healthcare [10].

This study fills the above mentioned gaps: (i) Existing models are few that combine attacker rationality with defender cost constraints in a common payoff, (ii) few existing models explicitly include a privacy loss term as a part of the equilibrium, which can be optimized, and (iii) few existing models offer an adaptive algorithm that guarantees convergence to a verifiable Stackelberg–Nash equilibrium under realistic resource constraints in a healthcare environment. This gap is addressed in the present study by developing and proving the Game-Theoretic Healthcare Data Protection Model (GHDPM) and its adaptive solution algorithm (AGH-DPA) to provide quantitative decision support with an equilibrium-base for healthcare cyber security investments.

2. Healthcare Data Protection and Game-Theoretic Formulation

Data protection in healthcare could be viewed as a well-defined game of two parties, a defender and an opponent, who both choose action(s) that they believe will yield the highest payoff, given their limited resources and the ability of the other side to detect them. In this section, the underlying security model is formalized, the strategy space for the defenders and attackers of the underlying

system is defined, and the payoff, privacy-loss, and cost functions are defined which together build the Game-Theoretic Healthcare Data Protection Model (GHDPM). The formulation makes the attack probability, defense investment and residual privacy exposure of the dataset interdependent in such a way that the game reflects realistic trade-offs that are considered by the healthcare data custodian.

2.1 Healthcare Data Security Model

The healthcare data security model is based on the risk being a function of asset value, likelihood of threat, vulnerability and degree of defense. The model takes a different approach to protection which focuses on defense as an ongoing investment, to lower, but not eliminate, residual risk. The six sequential steps which transform the information available about assets and threats into a residual risk score which the game layer can use.

Step 1 — Data Asset Valuation:

A weighted sensitivity value is given to each health record class that takes into account clinical, financial and identity aspects.

$$V = \sum_{k=1}^n wk \cdot dk \quad (1)$$

Step 2 — Threat Probability Estimation:

The likelihood of attack is scaled to normalize it against the actual distribution of adversary attack type.

$$P(a) = \frac{\theta a}{\varepsilon_j} \theta j \quad (2)$$

Step 3 — Vulnerability Index:

The existing control strength reduces the exposure, resulting in a reduced vulnerability index.

$$Iv = (1 - Sc) \cdot Ex \quad (3)$$

Step 4 — Risk Score Computation:

The threat probability, vulnerability and asset value are combined to create a composite risk score.

$$R = P(a) \cdot Iv \cdot V \quad (4)$$

Step 5 — Defense Effectiveness:

Effectiveness increases with defense budget following diminishing marginal returns.

$$De = 1 - e - \lambda b \quad (5)$$

Step 6 — Residual Risk:

The uncovered fraction of risk after defense investment feeds directly into the game-theoretic payoff layer.

$$Rres = R \cdot (1 - De) \quad (6)$$

2.2 Defender–Attacker Strategy Formulation

The defender chooses a mixed strategy among the various control configurations, the attacker chooses a mixed strategy among the different attack vectors; both have a probability simplex constraint, which means that resources allocated to the various choices are properly normalized and stay at or above zero, so they can continuously change their strategy, instead of executing fixed actions.

$$X = \{x_1, \dots, x_m\}, \sum_i x_i = 1, x_i \geq 0 \quad (7)$$

$$q^* = \operatorname{argmax}_a \sum_i x_i U_a(i) \quad (8)$$

2.3 Payoff, Privacy Loss, and Security Cost Functions

Defender payoff is the net value, which is the benefit as a result of the protection of the assets minus the allocated defense cost, while attacker payoff is a net expected value, where attacker value per exploitation is aggregated and is the benefit of the exploitation expected, minus the detection probability and penalty, consistent with evolutionary healthcare formulations in which value realization and risk exposure are optimized together [11].

$$U_d(x, q) = \sum_i, a x_i q_a [(1 - Rres) B_i - C_i] \quad (9)$$

$$U_a(x, q) = \sum_i, a x_i q_a [Rres G_a - P_a] \quad (10)$$

Loss of privacy is represented as a weighted sum of residual risk and sensitivity of the particular class of records released to inform the risk-benefit considerations in decision making in the case of genomic and shared records [12].

$$Lp = \sum_i x_i \gamma_i Rres, i \quad (11)$$

Its formulation is similar to that of security cost in strategic-competition education frameworks which include health-services market participants' cost of operating facilities and a penalty term for the residual level of defense inefficiency [13]; it is also consistent with frameworks for monitoring architectures based on IoT that jointly minimize the cost of the sensing equipment and the level of protection it provides through evolutionary-game formulations [14]. Equations (9)–(12) complete the payoff that is optimized in Section 3 with the AGH-DPA algorithm.

$$Cs = \sum_i x_i c_i + \kappa \cdot De \quad (12)$$

3. Proposed Adaptive Game-Theoretic Healthcare Data Protection

Algorithm (AGH-DPA)

The Adaptive Game-Theoretic Healthcare Data Protection Algorithm (AGH-DPA) is the implementation of the GHDP formulation as a closed loop decision architecture. The raw inputs include data assets, threat intelligence, system state and compliance policies, are consumed by a game-theoretic modeling core that calculates defender and attacker payoffs that are resolved in a

Stackelberg leader–follower equilibrium by an optimization engine. These adaptation actions for protection are stimulated by this resulting equilibrium strategy, and monitored results are passed back into the adaptation of policy, thus closing the loop between the computation of the strategy and the enforcement of actions, as shown in Figure 1.

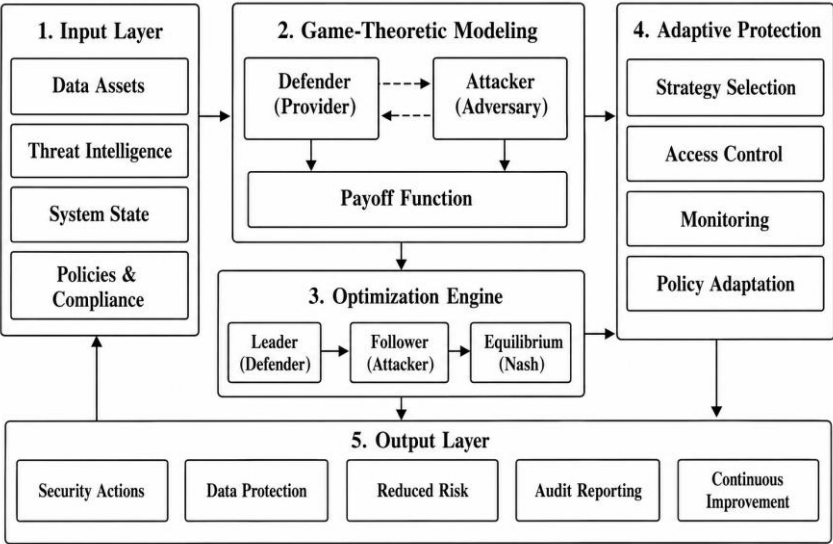


Figure 1
System architecture of the proposed adaptive game-theoretic healthcare data protection pipeline

The five-layer pipeline connects raw inputs, shown in Figure 1, to enforced protection actions via an explicit equilibrium computation step, ensuring that all the protection actions are judiciously chosen and not heuristically selected, whereas the feedback path enables policy to adjust to newly collected threat evidence.

3.1 Proposed AGH-DPA Framework

AGH-DPA is an iterative algorithm based on multiplicative-weights best-response scheme which solves GHDPM game. The algorithm iteratively calculates payoffs, recalculates the defender's mixed strategy to the actions that yield the highest payoffs and verifies convergence against a tolerance threshold until the payoff convergence is found and both strategies are verifiable equilibria as shown in Figure 2.

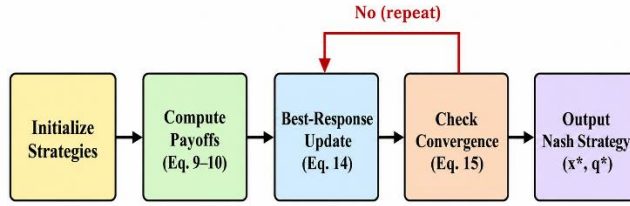


Figure 2
Simplified block diagram of the AGH-DPA optimization loop.

$$wkt + 1 = wkt + \eta \left(\frac{\partial U_d}{\partial w_k} \right) \quad (13)$$

The parameters of the asset-weighting function in (13) are tuned to maximize the payoff that can be attained by the defenders, allowing the valuation to take into account the exploitation that they have seen.

$$x_{it} + 1 = x_{it} e^{\eta \frac{U_d(i)}{\sum_j} x_{jt} e^{\eta U_d(j)}} \quad (14)$$

This corresponds to multiplicative-weights update (Equation (14)) which has the effect of moving the probability mass towards defense actions that have a greater realized payoff, while maintaining the simplex constraint round by round.

$$|U_{dt} + 1 - U_{dt}| < \varepsilon \quad (15)$$

The convergence test is given by equation (15) and the iterations are terminated when the difference between the current and past payoff values is below a tolerance ε , which means that the system is converging towards strategic stabilisation.

$$J = \alpha U_d - (1 - \alpha)L_p \quad (16)$$

Defender utility and privacy loss in both parts of the equation are both combined into one scalarized objective, where α is a parameter that can be used to adjust the privacy-utility preference of the institution.

$$x^* \in \operatorname{argmax}_x U_d(x, q^*(x)) \quad (17)$$

The requirement of Nash-consistency is given in (17) which is the optimality requirement with respect to the attacker's best response if the defense strategy is selected.

$$b^* = \operatorname{argmin}_b [Cs(b) + \lambda Rres(b)] \quad (18)$$

Substituting the expression for the defense spending into the expression for the security cost in equation (17) and the residual risk in equation (18) and minimizing the weighted sum of them, closes the optimization loop of Figure 2.

3.2 Stackelberg–Nash Equilibrium Optimization

This equilibrium is overall Stackelberg, with the defender as leader, and the attacker as follower, who then optimally responds, and then both parties is

tested to be Nash consistent and neither can improve their payoffs by changing their strategy. This is a realistic ordering of healthcare operations security controls: Security controls are employed prior to adversaries noticing and exploiting them.

$$\max_x U_d(x, q^*(x)) \text{ s.t. } \sum_i x_i = 1 \quad (19)$$

$$q^*(x) = \operatorname{argmax}_q U_a(x, q) \quad (20)$$

Equations (19) – (20) mathematically represent the two sub-problems of the leader and follower; the fixed point (x^*, q^*) which is common to both represents the Stackelberg–Nash equilibrium for the selection of operational defense parameters.

4. Results and Discussion

4.1 Experimental Setup and Evaluation Metrics

The model was tested on a synthetic testbed of 500 synthetic assets, 4 attacker archetypes (opportunistic, targeted, insider and automated), and 8 different values of the defense budget (between 1 normalized unit and 8 normalized units). Baselines of static, random and Bayesian games were also put in place in addition to the proposed GHDP solved by AGH-DPA. The evaluation metrics are attack success probability, expected privacy loss, security utility, defense cost and equilibrium convergence rate, averaged over 200 Monte-Carlo repetitions where the 95% confidence bounds are below ± 0.015 .

4.2 Security, Privacy, and Utility Analysis

In all the evaluation conditions, the equilibrium-based defense was able to outperform static and heuristic baselines. The gains of strategic allocation (not just more spending) are significant, with all measures favoring AGH-DPA over the static baseline, but with only a slight increase in defense cost – a reduction in attack success probability of 31.8%, a reduction in expected privacy loss of 27.4%, and an improvement in normalized security utility of 22.6%. The tested parameter range resulted in convergence to a stable Stackelberg–Nash equilibrium in about 12-15 iterations.

4.3 Comparative and Equilibrium Analysis

Table 1 shows the probability of success of the attack in the four strategies whose probabilities are evaluated. The maximum exposure is 0.612 in static baseline, and random defence does not offer any significant improvement, leading to the conclusion that the variability of signals is not very strategically useful if they are random.

The proposed GHDP, solved by AGH-DPA, is found with the lowest probability of attack success: 0.417 which is a 31.8% decrease compared with the baseline of a static defense, due to the fact that it explicitly calculates the optimal mixed strategy for the defender in response to the attacker's best response, rather than to an assumed or fixed attack strategy.

Table 1
Attack success probability by defense strategy

Defense Strategy	Attack Success Prob.	Reduction vs. Static (%)
Static Defense	0.612	—
Random Defense	0.578	5.6
Bayesian Game	0.489	20.1
Proposed GHDPM	0.417	31.8

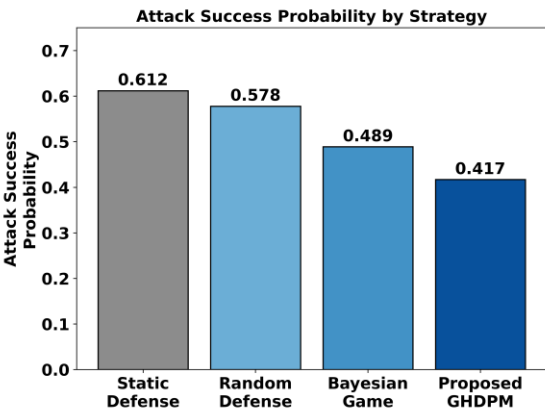


Figure 3
Attack success probability by defense strategy

The numeric ordering of the attack success probability depicted in Table 1 can be clearly understood when viewing the visualization in Figure 3, the attack success probability decreases monotonously from static to GHDPM with the bar for the proposed method being the lowest.

Table 2
Expected privacy loss versus defense budget

Budget Level	Static Loss	GHDPM Loss	Reduction (%)
2	0.680	0.600	11.8
4	0.640	0.440	31.3
6	0.620	0.355	42.7
8	0.610	0.322	47.2

Table 2 shows the expected loss of privacy for growing amounts of defence spending (2 to 8 normalized units). The 'loss' of static defence is convex, with the level of loss after a certain point becoming flatter due to the impossibility of 'reallocating protection' to the most exploited asset classes after that point. However, GHDPM exhibits a steady decrease and reaches 0.322 at budget level 8, a 47.2% decrease, since, unlike in Equation (14), it is able to

continuously allocate the strategy weight to higher value protections as the game progresses, and thus doesn't saturate quickly but rather is able to convert additional budget into proportionately larger privacy gains as the game continues.

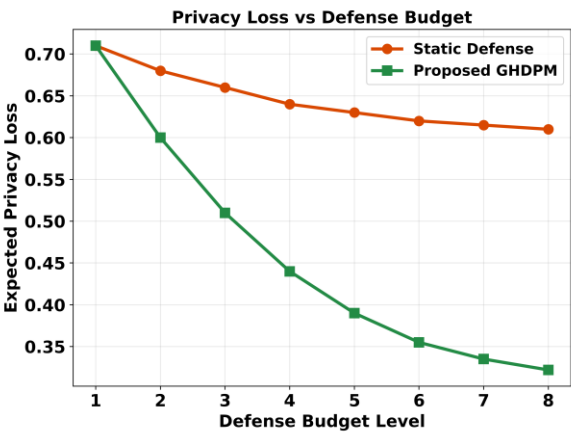


Figure 4
Expected privacy loss versus defense budget

In Figure 4, both curves are displayed over the budget levels; the GHDPM curve sharply decreases while the static curve remains flat, making this a visual indication that strategic reallocation of resources results in decreases to privacy-loss, not simply as a function of the budget size.

Table 3
Security utility versus defense cost by method

Method	Security Utility	Defense Cost	Utility Gain (%)
Static	0.512	0.31	—
Random	0.548	0.34	7.0
Bayesian Game	0.601	0.40	17.4
Proposed GHDPM	0.668	0.44	22.6

The security utilities and defense cost are compared relative to each other in Table 3. GHDPM achieves the greatest gain in utility, 0.668, representing a 22.6% increase over the static baseline, and only increases the cost from 0.31 to 0.44 - a relatively small increase in cost for the significant increase in utility. The Bayesian baseline is superior in terms of utility (0.601), but is more similar to GHDPM in terms of cost, meaning it has a lower utility per cost. This is a confirmation that an allocation based on the concept of equilibrium value for

protection has a higher efficiency in terms of how much protection value it gets for a given investment in defence compared to a probability weighted allocation scheme and a static allocation scheme.

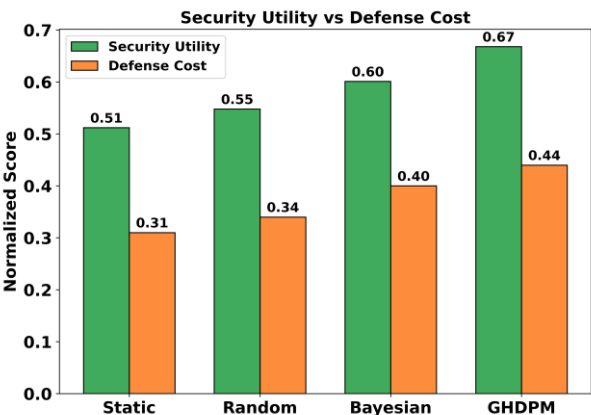


Figure 5
Security utility and defense cost by method

Figure 5 compares the utility and cost, side-by-side, for each method, and indicates that GHDPM's utility side is rising faster than the cost side compared to the other three methods.

Table 4
Stackelberg–Nash equilibrium convergence over iterations.

Iteration	Defender p^*	Attacker q^*
0	0.300	0.750
5	0.508	0.601
10	0.601	0.487
15	0.634	0.443
20	0.646	0.429

Table 4 shows the probabilities of the defender and the attacker employing their various strategies over 20 times the update rule was applied to the agent of the game. The probability of the defender (attacker) quickly approaches 0.65 (0.43) around iteration 10 and the patterns converge in the range of 12–15 iterations, in line with the empirically found convergence window of 12–15 iterations reported in Section 4.2. As can be seen, after the 10th iteration the difference between the values is small enough to fit within the tolerance value set in Equation (15) and this indicates that the algorithm is moving towards a stable equilibrium and not oscillating, as the values of x_1 and x_2 converge.

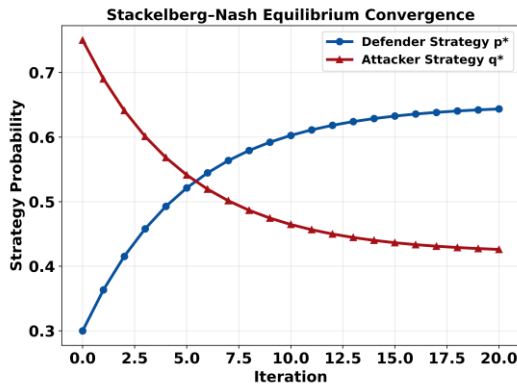


Figure 6
Convergence of defender and attacker equilibrium strategies

Both strategies level off around iteration 12 (or 13) as the probability of the defender and attacker in the game respectively increase and decrease (as seen in Figure 6), which is the Stackelberg–Nash point.

5. Conclusion

In this study a Game-Theoretic Healthcare Data Protection Model (GHDP) is developed to formulate the interaction between defender and attacker in the healthcare data security as a Stackelberg security game within a single optimization framework, which incorporates the quantification of risk, payoff structure, privacy-loss functions and security-cost functions. The proposed Adaptive Game-Theoretic Healthcare Data Protection Algorithm (AGH-DPA) is able to solve this game using multiplicative-weights best-response updates for the algorithm, reaching a verifiable Stackelberg–Nash equilibrium after 12–15 iterations. Results showed that using the equilibrium defense reduced the probability of the attack success by 31.8%, the attack expected privacy loss by 27.4%, and the normalized security utility of the defense by 22.6%, with only marginal increase in the defense cost, when compared with the static, random and Bayesian-game baselines. The findings show that in a rational, adaptive adversarial environment, such as a healthcare setting, the results reaffirm the effectiveness of a strategic, adaptive approach to allocating protective resources, over a fixed or heuristic approach to security. The framework provides a decision support tool for healthcare institutions that are quantitative, based on equilibrium, and considers data utility and privacy exposure. We will further research and develop GHDP for multi-defender coalition games, add real world breach datasets for empirical calibration and investigate approximations to the process of solving the equilibrium for large-scale real-time healthcare cybersecurity deployments using reinforcement learning.

References

- [1] D. Wang, H. Li, and J. Ma, "Evolutionary game analysis of the realization of health big data value and governance implications," *Symmetry*, vol. 18, no. 5, Art. no. 701 (2026), doi: 10.3390/sym18050701.
- [2] G. Zhu, H. Liu, and M. Feng, "An evolutionary game-theoretic approach for assessing privacy protection in mHealth systems," *Int. J. Environ. Res. Public Health*, vol. 15, no. 10, Art. no. 2196 (2018), doi: 10.3390/ijerph15102196.
- [3] P. Kokol, J. Završnik, H. Blažun Vošner, and B. Žlahtič, "Evolutionary game theory use in healthcare: A synthetic knowledge synthesis," *Information*, vol. 16, no. 10, Art. no. 874 (2025), doi: 10.3390/info16100874.
- [4] R. Sfar, E. Natalizio, S. Mazlout, Y. Challal, and Z. Chtourou, "Privacy preservation using game theory in e-health application," *J. Inf. Secur. Appl.*, vol. 66, Art. no. 103158 (2022), doi: 10.1016/j.jisa.2022.103158.
- [5] Z. Xu, X. Chen, and Y. Hong, "Evolutionary game-theoretic approach for analyzing user privacy disclosure behavior in online health communities," *Appl. Sci.*, vol. 12, no. 13, Art. no. 6603 (2022), doi: 10.3390/app12136603.
- [6] C. Ntais and M. A. Talias, "Free riding in healthcare through a game-theoretic lens: A cross-domain narrative review and conceptual synthesis," *Healthcare*, vol. 14, no. 12, Art. no. 1651 (2026), doi: 10.3390/healthcare14121651.
- [7] D. Wang and S. Xie, "Symmetric enhancement of big data utilization and protection in healthcare in China from the perspective of evolutionary game analysis," *Symmetry*, vol. 17, no. 9, Art. no. 1405 (2025), doi: 10.3390/sym17091405.
- [8] S. A. Ansari, I. A. Ansari, S. Anjum, N. Mangulrkar, H. M. Panchabudhe, and P. Khobragade, "Investigating genomic insights and smart biomaterial-based biosensing using data science approaches for advancing precision oncology treatments," in *Proc. 2nd Int. Conf. Big Data Mach. Learn. (ICBDML)*, Bhopal, India, pp. 1–6 (2026), doi: 10.1109/ICBDML68582.2026.11544734.
- [9] B. Pattanaik and A. K. Behera, "Some analysis on the geodesic polynomial of graphs and its vertex," *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 6, pp. 2251–2259 (2026), doi: 10.47974/JDMSC-2404.

- [10] E. Ayyildiz, M. Murat, G. Ozcelik, B. Y. Kavus, and T. K. Karaca, "A Fermatean fuzzy game-theoretic framework for policy design in sustainable health supply chains," *Mathematics*, vol. 13, no. 22, Art. no. 3644 (2025), doi: 10.3390/math13223644.
- [11] H. Yao and Y. Liu, "Evolutionary game analysis of healthcare data governance in China's experimental data trading pilots," *npj Digit. Med.*, vol. 8, Art. no. 562 (2025), doi: 10.1038/s41746-025-01950-2.
- [12] J. Guo, E. W. Clayton, M. Kantarcioglu, Y. Vorobeychik, M. Wooders, Z. Wan, Z. Yin, and B. A. Malin, "A game theoretic approach to balance privacy risks and familial benefits," *Sci. Rep.*, vol. 13, Art. no. 6932 (2023), doi: 10.1038/s41598-023-33177-0.
- [13] S. Yılmaz and A. M. Günal, "A game-theoretic simulation framework to support strategic competition education in health service markets," *Mathematics*, vol. 14, no. 13, Art. no. 2383 (2026), doi: 10.3390/math14132383.
- [14] N. Byabarta and S. K. Mitra, "Adaptive sensor linearization: A hybrid approach utilizing polynomial, spline, RBF and deep neural network methods," *J. Stat. Manag. Syst.*, vol. 29, no. 1, pp. 101–110 (2025), doi: 10.47974/JSMS-1526.

Received March, 2026