[1,2]Mohamed Ayari*

[1]Saleh M. Altowaijri

[1]Ahmed Alhomoud

A Novel Approach Based on Game Theory for Data Security Improvement

Journal of Electrical Systems

Abstract: - In the ever-evolving landscape of Information and Communication Technology (ICT), ensuring robust data security remains a pivotal challenge. As cyber threats grow in sophistication and frequency, traditional security mechanisms often fall short of effectively safeguarding data against unauthorized access and cyber-attacks. This research introduces a novel approach rooted in game theory, specifically leveraging the Nash equilibrium concept, to enhance data security frameworks. By analyzing the strategic interactions between potential attackers and defenders, this study aims to develop a dynamic, predictive model that adapts to changes in threat landscapes. The proposed method promises not only to bolster the confidentiality, integrity, and availability of data but also to revolutionize the existing paradigms of cybersecurity and network privacy. This groundbreaking approach is expected to make significant contributions to the fields of cybersecurity, offering a strategic edge in the ongoing battle against digital threats.

Keywords: Data Security; Game Theory; Nash Equilibrium; Cybersecurity Strategy; ICT

I. INTRODUCTION

In the contemporary digital ecosystem, the imperative for robust data security mechanisms cannot be overstated. Information and Communication Technology (ICT) systems form the backbone of global communications and data exchange, making them prime targets for cyber threats. Traditional security measures, while foundational, are increasingly being outmaneuvered by sophisticated cyber-attacks, prompting a shift towards more dynamic and predictive security frameworks. Recognizing the limitations of existing strategies, this research introduces a novel approach utilizing game theory to enhance cybersecurity measures effectively. Recent studies, such as those by Cuong et al. [1], highlight the application of game-theoretic approaches in cybersecurity, emphasizing the strategic interaction between attackers and defenders. Social media networks, as discussed by Cuong et al. [1], and cloud computing environments, explored by Wu et al. [2], present complex security challenges due to the massive centralization of user data and the extensive use of shared resources, respectively. These environments are susceptible to insidious attacks that not only compromise data integrity but also infringe upon user privacy. Moreover, the rapid advancement and integration of Internet of Things (IoT) devices further complicates the security landscape, as noted in works by Duan et al. [3] and Hamdi and Abie [4]. This research builds upon foundational theories introduced by Kroll et al. [5] on the governance of Bitcoin and extends to the protective measures against attacks in decentralized systems. The application of Nash equilibrium concepts, as proposed in our approach, is designed to optimize security strategies in a manner that is both anticipatory and adaptive to potential threats. The main contribution of this study lies in its innovative use of game theory to develop a security model that not only anticipates potential threats but also dynamically adapts to ongoing and evolving security challenges. Our approach, which integrates insights from multiple domains—including social media [6-10], cloud computing [11-21], and IoT [2-3] [22-24]—provides a comprehensive framework that enhances the predictability and effectiveness of cybersecurity measures. Further, the research addresses the limitations noted in existing studies, such as those by Chung et al. [25], who investigated the efficacy of Q-Learning in secure systems management. By implementing a game-theoretic model that accounts for various adversarial behaviors and potential collaborations among malicious entities, as explored by Agarwal [10] and others [13-21], our model represents a significant advancement in the theoretical and practical aspects of cybersecurity. This introduction sets the stage for a detailed discussion on the theoretical underpinnings of game theory in cybersecurity, the

[1*]Corresponding author: Mohamed.ayari@nbu.edu.sa

[1]Faculty of Computing and Information Technology, Northern Border University –Kingdom of Saudi Arabia

[2]Syscom Laboratory, National Engineering School of Tunis, University of Tunis El-Manar, Tunisia

development of our strategic model based on Nash equilibrium, and an analysis of its implementation across various ICT platforms. Through this study, we aim to contribute a substantial advancement to the field of cybersecurity, offering a strategic, efficient, and adaptable solution to the complex challenges of modern digital security.

The paper is structured as follows: Section 2 explores the theoretical background of game theory. Section 3 provides a detailed mathematical foundation of the approach based on Nash Equilibrium, its application in cybersecurity, and the presentation and discussion of the numerical analysis and simulation results. Finally, Section 4 concludes our work.

II. GAME THEORY

Game theory is a branch of mathematics that studies strategic interactions among rational decision-makers. It offers a structure for examining situations in which the result for each player is influenced by the behavior of all individuals involved. This section outlines the mathematical foundations of game theory, discussing its key concepts and types, setting the stage for its application in various domains, including cybersecurity.

II.1 Key Concepts in Game Theory

Game theory offers a systematic method for comprehending the strategic interactions among rational decision-makers. This section explores the fundamental concepts that form the backbone of game theory.

Players

Players are the individuals who have the authority to make choices and determine the sequence of action in a game. Each player aims to maximize their own payoff by selecting strategies that yield the best possible outcomes for themselves. In a game, players can be individuals, companies, or any entities capable of making strategic decisions. The interaction between these players determines the overall dynamics and outcomes of the game.

For example, in a cybersecurity context, players might include a network defender (such as an IT administrator) and an attacker (such as a hacker). Each player will have specific goals: the defender aims to protect the network, while the attacker aims to breach it.

Strategies

Strategies are thorough and systematic plans that players follow consistently throughout the whole game. It determines the player's behavior at every conceivable choice point. There exist two primary categories of strategies:

- **Pure Strategies**: These involve choosing a specific action with certainty. For instance, a defender might always choose to install a particular security software as a pure strategy.
- **Mixed Strategies**: These involve selecting actions probabilistically. For example, a defender might choose to install different security software with certain probabilities to make it harder for the attacker to predict their actions.

In a game, the strategy set S_i for player *i* encompasses all possible strategies that player can adopt. The choice of strategy significantly influences the game's outcome.

Payoffs

Payoffs are the outcomes received by players as a result of the combination of chosen strategies. They quantify the benefit or loss to each player and are represented by a payoff function. The payoff function $u_i(s_1, s_2 \cdots, s_n)$ for player *i* is contingent upon the strategies $s_1, s_2 \cdots, s_n$ selected by all players.

For example, in a cybersecurity scenario, the defender's payoff might represent the level of security achieved or the costs saved from preventing an attack, while the attacker's payoff might reflect the success of the attack, or

the resources expended.

II.2 Categories of Games

Game theory involves a wide variety of games, each with distinct characteristics and rules that involve various strategic interactions and decision-making processes. Understanding these types is essential for applying game theory to diverse scenarios, including economics, political science, and cybersecurity. This section delves into the primary types of games: static (simultaneous) games, dynamic (sequential) games, zero-sum games, and non-zero-sum games.

1- Simultaneous Games

Sometimes known as static games, are a type of game where players make their decisions in parallel, without any information about the choices made by other players. Usually, these games are depicted in a standard format called normal form, where a reward matrix is employed to present the results for every possible combination of strategies.

Characteristics:

- **Simultaneity**: Players choose their strategies at the same time.
- **Normal Form Representation**: Outcomes are displayed in a matrix where each cell contains the payoffs for the corresponding strategies.
- **Strategic Interdependence**: refers to a situation where the outcome for each participant is influenced by the strategies adopted by all participants.
- The outcome (payoff) for each player is determined by the strategies used by all players.

Example: Let's examine the situation where two companies are making a decision on whether or not to enter a new market. Each firm's profit depends on whether the other firm enters the market or stays out. The decision matrix shows the payoffs for each combination of strategies.

2- Dynamic (Sequential) Games

Dynamic games involve players making decisions at different points in time, allowing them to react to previous actions. These games are represented in extensive form, using a game tree to illustrate the sequence of moves and corresponding payoffs.

Characteristics:

- **Sequential Decision-Making**: Players make decisions one after another, with knowledge of previous actions.
- **Extensive Form Representation**: The game is depicted as a tree, with nodes representing decision points and branches representing actions.
- **Backward Induction**: A method employed to resolve dynamic games through examining the game starting with the final stage and selecting the best possible choices at each preceding stage.

Example: Consider a scenario where a government decides on a regulatory policy, and companies subsequently decide on investment levels based on the regulation. The game tree represents the sequence of decisions and their impacts.

3- Zero-Sum Games

Zero-sum games are competitive situations in which any gain made by one player is exactly offset by the loss experienced by the other player. The aggregate payment for all participants remains consistent, resulting in a

cumulative sum of payoffs equal to zero.

Characteristics:

- **Strict Competition**: The acquisition of one player corresponds to the loss of another player.
- **Constant Total Payoff**: The aggregate of the payoffs for all players is zero.
- **Applications**: Often used in competitive fields such as sports, military strategy, and certain economic models.

Example: An illustrative instance is a game of chess, in which the victory of one player corresponds to the defeat of the other player. The total outcome for both players is a constant sum.

4- Non-Zero-Sum Games

The aggregate payout in non-zero-sum games for all participants is variable; and the interests of players are not completely conflicting. These games facilitate the potential for mutual advantage and collaboration.

Characteristics:

- **Potential for Cooperation**: Players can achieve better outcomes through collaboration.
- **Variable Total Payoff**: The sum of the payoffs can vary, allowing for win-win situations.
- **Applications**: Common in economics, business, and social interactions where cooperation can lead to improved outcomes.

Example: Consider two firms deciding whether to form a partnership. By collaborating, they can achieve higher profits than they would individually. The payoff matrix reflects the potential for mutual benefit.

5- Bayesian Games

Bayesian games involve players with incomplete information about other players. Each player has beliefs about the probability distribution of the possible types or strategies of other players, and they update these beliefs based on observed actions.

Characteristics:

- **Incomplete Information**: Players do not have full knowledge of the other players' strategies or types.
- **Beliefs and Updates**: Players form and update beliefs about the unknowns based on observed actions.
- **Applications**: Used in scenarios where players must make decisions with uncertain or incomplete information, such as auctions and market competitions.

Example: In an auction, bidders do not know each other's valuations of the item but have beliefs about these valuations. They update their strategies based on observed bids to maximize their payoff.

6- Repeated Games

Repeated games involve players interacting multiple times, allowing strategies to evolve based on past interactions. These games can model long-term relationships and ongoing strategic interactions.

Characteristics:

- **Multiple Rounds**: Players engage in the game repeatedly over several periods.

- **Strategy Evolution**: Players can adjust their strategies based on outcomes of previous rounds.

- **Applications**: Used to analyze long-term interactions in economics, political negotiations, and business practices.

Example: Consider a repeated interaction between a supplier and a retailer. Over time, they may develop strategies that foster long-term cooperation, such as agreeing on fair prices and delivery schedules.

Overall, Game theory offers a structured approach to examining strategic interactions across different scenarios, offering unique insights and tools for decision-making. This knowledge is crucial for applying game theory to complex scenarios, like cybersecurity.

II.3 Normal Form Representation (NFR)

The normal form representation (NFR) is a method of depicting static (simultaneous) games by means of a matrix that displays the payoffs for each player over all potential strategy combinations. This mode of representation is especially advantageous for evaluating games in which players make simultaneous decisions, unaware of the strategies used by their counterparts.

Key Characteristics of Normal Form Representation

1. **Players**:
   - The decision-makers involved in the game.
   - Each player possesses a repertoire of strategies from which they can select.
2. **Strategies**:
   - The possible actions that each player can take.
   - Represented as rows and columns in the payoff matrix.
3. **Payoffs**:
   - The outcomes that result from each combination of strategies.
   - Each cell in the matrix contains a pair (or set) of payoffs, one for each player.

Example of a Normal Form Game

Consider a game with two companies, Company A and Company B, each deciding whether to launch an advertising campaign (Advertise) or not (Don't Advertise).

Strategies:

- Company A: Advertise (A), Don't Advertise (NA)
- Company B: Advertise (A), Don't Advertise (NA)

Table1: Example of NFR Payoff Matrix

	Company B: Advertise (A)	**Company B: Don't Advertise (NA)**
Company A: Advertise (A)	(10, 10)	(15, 5)

Company A: Advertise (NA)	**Don't**	(5, 15)	(0, 0)

In this matrix:

- If both companies advertise, they share the market equally, resulting in payoffs of (10, 10).
- If Company A advertises and Company B does not, Company A gains a larger market share, resulting in payoffs of (15, 5).
- If Company B advertises and Company A does not, Company B gains a larger market share, resulting in payoffs of (5, 15).
- If neither company advertises, both maintain their current market share, resulting in payoffs of (0, 0).

Analysis Using Normal Form Representation

1. **Dominant Strategy**:
   - A dominant strategy is one that guarantees a higher return for a player, regardless of the strategy chosen by the opponent.
   - In this example, if both companies have a dominant strategy to advertise, they will choose to do so.
2. **Nash Equilibrium**:
   - A collection of strategies in which no participant may gain an advantage by independently altering their approach.
   - In this case, the Nash Equilibrium is reached once the two companies choose to promote, resulting in payoffs of (10, 10).

The normal form representation simplifies the analysis of static games, making it easier to identify optimal strategies and predict outcomes.

2.4 Extensive Form Representation (EFR)

Extensive form representation is used to describe dynamic (sequential) games where players make decisions at different points in time. This form of representation is depicted as a tree, illustrating the sequence of moves, decision points, and the corresponding payoffs.

Key Characteristics of Extensive Form Representation

1. **Decision Nodes**:
   - Points in the game where a player must choose a strategy.
   - Represented as vertices (nodes) in the tree.
2. **Branches**:
   - The possible actions a player can take at each decision node.
   - Represented as edges (branches) connecting the nodes.
3. **Payoffs**:

- The outcomes that result from a sequence of actions.
- Represented at the terminal nodes (leaves) of the tree.

Example of an Extensive Form Game

Consider a sequential game involving two companies, Alpha and Beta, deciding on market entry strategies.

1. **Alpha** moves first and decides whether to enter a new market (Enter) or stay out (Stay).
2. **Beta** observes Alpha's decision and then decides whether to enter the market (Enter) or stay out (Stay).

The payoffs for each combination of actions are as follows:

- If Alpha enters and Beta enters, the payoffs are (3, 2).
- If Alpha enters and Beta stays out, the payoffs are (5, 0).
- If Alpha stays out and Beta enters, the payoffs are (0, 4).
- If both stay out, the payoffs are (1, 1).

Game Tree Representation:

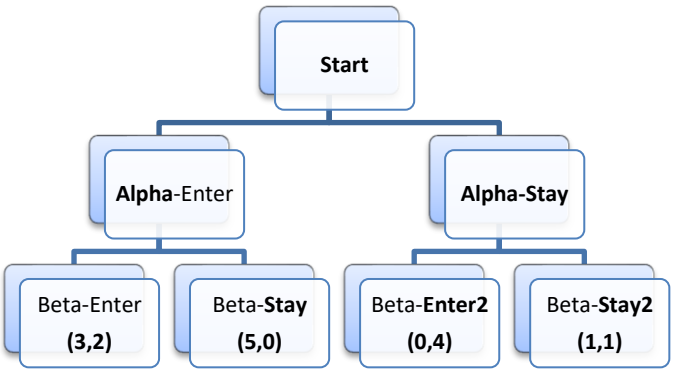

Figure 1- Game Tree Representation using EFR

In this tree:

- If Alpha enters (Enter) and Beta enters (Enter), the payoffs are (3, 2).
- If Alpha enters (Enter) and Beta stays out (Stay), the payoffs are (5, 0).
- If Alpha stays out (Stay) and Beta enters (Enter), the payoffs are (0, 4).
- If Alpha stays out (Stay) and Beta stays out (Stay), the payoffs are (1, 1).

In summary, the comprehensive form representation provides a visual depiction of the sequential decision-making process in dynamic games, which helps in determining the optimal tactics through the use of backward induction. The utilization of this approach is of utmost importance in comprehending intricate interconnections, particularly in the context of cybersecurity situations, and is implemented in subsequent sections.

III. NOVEL GAME-THEORETIC APPROACH BASED ON NASH EQUILIBRIUM

Nash Equilibrium is a fundamental concept in game theory that offers a powerful tool for evaluating strategic interactions in which the decisions made by each player have an impact on the outcomes of others. This section explores the detailed mathematical foundation of Nash Equilibrium and its application in developing a novel

game-theoretic approach for cybersecurity.

3.1 Mathematical Foundation of Nash Equilibrium

Nash Equilibrium is a situation in a game where no player can improve their position by changing their strategy alone, assuming that the strategies of the other players stay the same. This concept can be expressed mathematically in the following manner.

Definition: Nash Equilibrium

Consider a game with ***n*** players, where each player ***i*** has a strategy set S_i and a payoff function u_i:

$S_1 \times S_2 \times \cdots \times S_n \rightarrow \mathbb{R}$. A strategy profile $(s_1^*, s_2^*, \cdots, s_n^*)$ is a Nash Equilibrium if, for every player *i*,

$$u_i(s_i^*, s_{-i}^*) \geq u_i(s_i, s_{-i}^*) \qquad \forall s_i \in S_i \quad (1)$$

where s_{-i}^* denotes the strategy profile of all players except player *i*.

Put simply, in Nash Equilibrium, no player can enhance their payoff by deviating from their equilibrium strategy provided the other players maintain their plans unchanged.

Nash Equilibrium in a Two-Player Game

Consider a simple two-player game where each player has two strategies. The payoff matrix for the game is given by:

Table2: Payoff Matrix for Two-Players

	Player 2: A	**Player 2: B**
Player 1: A	(2, 2)	(0, 1)
Player 1: B	(1, 0)	(3, 3)

To find the Nash Equilibrium, we evaluate the optimal reaction of each player to the strategies employed by the other player.

1. **Optimal Responses from Player 1**:

- If Player 2 selects option A, Player 1's optimal reaction is also to select option A (since 2 > 1).
- If Player 2 selects option B, Player 1's optimal strategy is also to select option B (since 3 > 0).

2. **Optimal Responses from Player 2**:

- If Player 1 selects option A, Player 2's optimal strategy is to select option A (since 2 > 0).
- If Player 1 selects option B, Player 2's optimal strategy is to select option B (since 3 > 1).

The strategy profile ***(B, B)*** is a Nash Equilibrium because both players are choosing their best responses: Player 1 cannot improve by switching to A, and Player 2 cannot improve by switching to A.

3.2 Nash Equilibrium in Cybersecurity

The Nash Equilibrium notion has broad applicability across diverse domains, encompassing political science, economics, and cybersecurity. In the context of cybersecurity, Nash Equilibrium can be utilized to model and investigate the strategic exchanges between defenders and attackers, leading to more effective security strategies.

In cybersecurity, defenders and attackers are engaged in a strategic game where each party's actions influence the overall security landscape. Nash Equilibrium can help identify optimal strategies for both defenders and attackers, ensuring that the system is robust against potential threats.

First scenario: Defending Against Cyber Attacks

Consider a scenario where a network administrator (defender) must allocate resources to protect multiple assets, while a hacker (attacker) decides which asset to attack. Each player has two strategies:

- **Defender**: Allocate resources to Asset A (A1) or Asset B (A2).
- **Attacker**: Attack Asset A (A1) or Asset B (A2).

The payoff matrix is as follows:

Table3: Payoff Matrix for Defender-Attacker

	Attacker: A1	**Attacker: A2**
Defender: A1	(5, -5)	(2, -2)
Defender: A2	(1, -1)	(4, -4)

In order to determine the Nash Equilibrium, we examine the optimal strategy for each player.

1. **Defender's Best Responses**:
   - If the attacker chooses A1, the defender's best response is to allocate resources to A1 (since 5 > 1).
   - If the attacker chooses A2, the defender's best response is to allocate resources to A2 (since 4 > 2).
2. **Attacker's Best Responses**:
   - If the defender allocates resources to A1, the attacker's best response is to attack A2 (since -2 > -5).
   - If the defender allocates resources to A2, the attacker's best response is to attack A1 (since -1 > -4).

In this particular instance, a pure strategy Nash Equilibrium is absent due to the presence of cyclical patterns resulting from the optimal replies. Nonetheless, it is possible to identify a Nash Equilibrium in which players employ a mixed strategy by randomizing their choices according to specific probabilities.

To find the combined strategy Nash Equilibrium, suppose p the probability that the defender allocates resources to A1, and q be the probability that the attacker attacks A1.

The expected payoffs for the defender are:

- When allocating resources to A1: $E_u(D|A1) = 5q + 2(1-q) = 3q + 2$ (2)
- When allocating resources to A2: $E_u(D|A2) = 1q + 4(1-q) = -3q + 4$ (3)

For the defender to be indifferent between the two strategies, the expected payoffs must be equal:

$$3q + 2 = -3q + 4 \quad (4)$$

It yields:

$$q = {}^{1}/_{3} \quad (5)$$

The expected payoffs for the attacker are:

- When attacking A1: $E_u(A|A1) = -5p - 1(1-p) = -4p - 1$ (6)
- When attacking A2: $E_u(A|A2) = -2p - 4(1-p) = 2p - 4$ (7)

For the attacker to be indifferent between the two strategies, the expected payoffs must be equal:

$-p - 1 = 2p - 4$ (8)

It yields:

$p = {}^{1}/_{2}$ (9)

Thus, the mixed strategy Nash Equilibrium is:

- Defender allocates resources to A1 with probability $p = {}^{1}/_{2}$ and to A2 with probability $1 - p = {}^{1}/_{2}$.
- Attacker has a probability of $q = {}^{1}/_{3}$ to attack A1 and a probability of $1 - q = {}^{2}/_{3}$ to attack A2.

This equilibrium guarantees that both the defender and the attacker are employing the most effective techniques, hence enhancing the system's resilience against cyber-attacks.

Second Scenario: Protecting Critical Infrastructure from Multi-Vector Attacks

Consider a more complex scenario involving multiple assets and a variety of attack strategies. We will model a cybersecurity game between an organization (defender) with three critical assets and a hacker (attacker) who can choose among several attack strategies.

The following table summarizes the complex scenario:

Table4: Second Scenario Summary

Aspect	Details
Assets	Three critical systems: Asset A (A1), Asset B (A2), Asset C (A3)
Defender's Strategies	1. Invest heavily in Asset A (Invest-A) 2. Invest heavily in Asset B (Invest-B) 3. Invest heavily in Asset C (Invest-C) 4. Spread investments equally across all assets (Invest-All)
Attacker's Strategies	1. Attack Asset A (Attack-A) 2. Attack Asset B (Attack-B) 3. Attack Asset C (Attack-C) 4. Attack both Asset A and B (Attack-AB) 5. Attack both Asset B and C (Attack-BC) 6. Attack both Asset A and C (Attack-AC) 7. Attack all three assets (Attack-All)

Payoff Matrices

The payoffs are determined based on the success or failure of the attacks and the level of defense:

Table 5: Defender's Payoff Matrix:

	Attack-A	Attack-B	Attack-C	Attack-AB	Attack-BC	Attack-AC	Attack-All
Invest-A	-8	-2	-2	-10	-5	-5	-12
Invest-B	-2	-8	-2	-10	-5	-5	-12
Invest-C	-2	-2	-8	-10	-5	-5	-12
Invest-All	-6	-6	-6	-9	-9	-9	-15

Table 6: Attacker's Payoff Matrix:

	Attack-A	Attack-B	Attack-C	Attack-AB	Attack-BC	Attack-AC	Attack-All
Invest-A	8	-1	-1	9	4	4	11
Invest-B	-1	8	-1	9	4	4	11
Invest-C	-1	-1	8	9	4	4	11
Invest-All	7	7	-3	8	3	3	10

Nash Equilibrium Analysis and Interpretation

Based on the provided payoff matrices, the simulation results reveal the following Nash Equilibrium strategies:

Defender Strategies at Nash Equilibrium:

- Strategy 1: Invest heavily in Asset A (Invest-A)
- Strategy 2: Invest heavily in Asset B (Invest-B)
- Strategy 3: Invest heavily in Asset C (Invest-C)

Attacker Strategies at Nash Equilibrium:

- Strategy 7: Attack all three assets simultaneously (Attack-All)

These outcomes indicate that the defender's optimal strategies involve concentrating resources on individual assets, while the attacker's optimal strategy is to target all three assets at once.

Referring to the payoff matrices, Figure 2 illustrates the Defender_Payoff and Attacker_Payoff matrices. The left subplot shows the defender's payoff matrix with red dots marking the Nash Equilibrium points, while the right subplot shows the attacker's payoff matrix with black dots indicating the Nash Equilibrium points. The color intensity in the maps represents the magnitude of payoffs, aiding in the identification of regions with high and low payoffs.

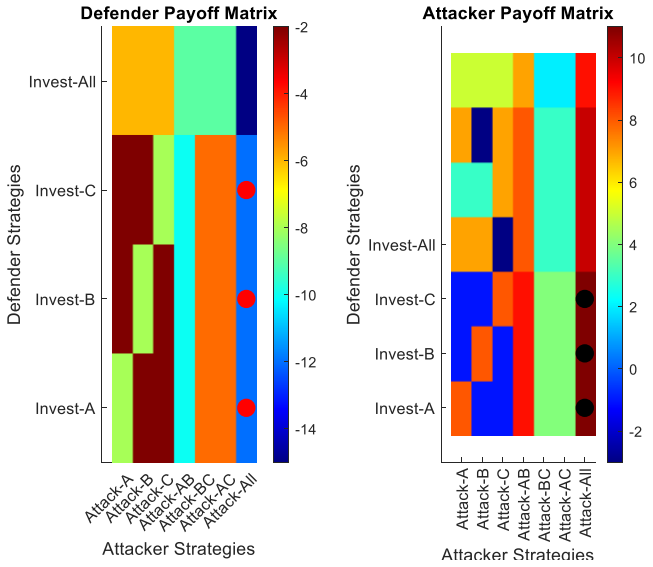

Figure 2- Payoff maps for Defender and Attacker Strategies

Figure 3 presents the payoff curves for both the defender and the attacker across various strategies. These curves show how payoffs change as players adjust their strategies. The Nash Equilibrium points are marked on these

curves, highlighting the optimal strategies where both players maximize their respective payoffs.

Key observations from the payoff curves include that the defender's strategies (Invest-A, Invest-B, and Invest-C) yield different payoffs depending on the attacker's strategy. The equilibrium points suggest that the defender can choose any of these strategies, as they all form part of the Nash Equilibrium. The attacker's strategy (Attack-All) consistently yields the highest payoff across the defender's strategies. This equilibrium point indicates that the attacker maximizes their payoff by attacking all assets simultaneously, regardless of the defender's specific investment.

These findings offer valuable insights for enhancing data security. The defender should focus resources on specific critical assets rather than spreading investments too thinly. This targeted approach can effectively counter multi-vector attacks, as the equilibrium strategies indicate. Given that attackers are likely to target all assets simultaneously, defenders must develop comprehensive security measures to protect all critical assets. This includes implementing robust security protocols and regular updates to safeguard against potential breaches.

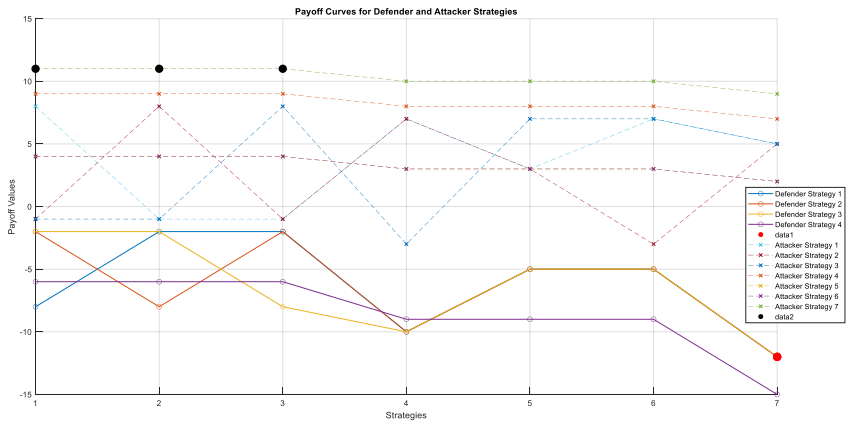

Figure 3- Payoff Curves for Defender and Attacker Strategies

The mixed strategy approach highlights the importance of dynamic defense mechanisms that can adapt to different attack vectors. By varying their defensive strategies, defenders can create uncertainty for attackers, making it more difficult for them to predict and exploit vulnerabilities.

The analysis underscores the need for proactive threat mitigation strategies. Defenders should continuously monitor their systems, conduct threat assessments, and update their defenses based on the latest intelligence about potential attack strategies. Organizations can use the insights from Nash Equilibrium to strategically plan and allocate their cybersecurity budgets. By understanding the optimal strategy for both defense and attack, Organizations can make well-informed decisions regarding the allocation of resources for security infrastructure and technology.

The study uses Nash Equilibrium to analyze cybersecurity strategic interactions between defenders and attackers. It emphasizes the importance of resource allocation, defense strategies, and proactive threat mitigation for securing critical assets. The approach helps organizations enhance data security measures and protect against sophisticated cyber-attacks. Visualizations demonstrate the robustness of the method, providing valuable information on defensive and offensive strategies.

VI CONCLUSION

This study presented a novel approach for ensuring data security using game theory, particularly the idea of Nash Equilibrium. We have created an advanced model for cybersecurity that is dynamic and adaptive by studying the strategic interactions between attackers and defenders. The results indicate that defenders should allocate efforts towards protecting vital assets, whereas attackers typically aim to exploit all assets simultaneously. By implementing a focused defense strategy and actively mitigating threats, it is possible to effectively combat attacks

that come from multiple sources. The study demonstrates the tangible implementation of Nash Equilibrium in the field of cybersecurity, highlighting the significance of focused resource distribution, all-encompassing defense tactics, and proactive threat reduction. The results offer significant perspectives for organizations to strategically devise and distribute their cybersecurity budgets. To summarize, utilizing game theory and Nash Equilibrium provides a strong framework for enhancing data security. This method has the potential to completely transform the way cybersecurity is approached, giving a strategic advantage in defending against advanced cyber-attacks and improving overall data security.

ACKNOWLEDGMENT

The authors gratefully acknowledge the approval and the financial support of this research from the Deanship of Scientific Research study by the grant number ***CSCR-2023-12-2253***, Northern Border University, Arar, KSA.

REFERENCE:

[1] Do, C. T., Tran, N. H., Hong, C., Kamhoua, C. A., Kwiat, K. A., Blasch, E., ... & Iyengar, S. S. (2017). Game theory for cyber security and privacy. *ACM Computing Surveys (CSUR)*, *50*(2), 1-37.

[2] Wu, Y., Lyu, Y., & Shi, Y. (2019). Cloud storage security assessment through equilibrium analysis. *Tsinghua Science and Technology*, *24*(6), 738-749.

[3] Duan, J., Gao, D., Yang, D., Foh, C. H., & Chen, H. H. (2014). An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications. *IEEE Internet of Things Journal*, *1*(1), 58-69.

[4] Hamdi, M., & Abie, H. (2014, June). Game-based adaptive security in the Internet of Things for eHealth. In *2014 IEEE international conference on communications (ICC)* (pp. 920-925). IEEE.

[5] Kroll, J. A., Davey, I. C., & Felten, E. W. (2013, June). The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In *Proceedings of WEIS* (Vol. 2013, No. 11).

[6] Rodrigues, A., Villela, M. L., & Feitosa, E. (2024). A Systematic Mapping Study on Social Network Privacy: Threats and Solutions. *ACM Computing Surveys*.

[7] Hang, P., Lv, C., Xing, Y., Huang, C., & Hu, Z. (2020). Human-like decision making for autonomous driving: A noncooperative game theoretic approach. *IEEE Transactions on Intelligent Transportation Systems*, *22*(4), 2076-2087.

[8] Megías, D., Kuribayashi, M., & Qureshi, A. (2020). Survey on decentralized fingerprinting solutions: Copyright protection through piracy tracing. *Computers*, *9*(2), 26.

[9] Jain, L., Katarya, R., & Sachdeva, S. (2020). Recognition of opinion leaders coalitions in online social network using game theory. *Knowledge-Based Systems*, *203*, 106158.

[10] Agarwal, P., Al Aziz, R., & Zhuang, J. (2022). Interplay of rumor propagation and clarification on social media during crisis events-A game-theoretic approach. *European Journal of Operational Research*, *298*(2), 714-733.

[11] Saadatfar, H., Gholampour Ahangar, H., & Hassannataj Joloudari, J. (2024). A New Dynamic Game-Based Pricing Model for Cloud Environment. *Future Internet*, *16*(2), 49.

[12] Patra, M. K., Sahoo, S., Sahoo, B., & Turuk, A. K. (2019, December). Game theoretic approach for real-time task scheduling in cloud computing environment. In *2019 International Conference on Information Technology (ICIT)* (pp. 454-459). IEEE.

[13] Gao, L., Yan, Z., & Yang, L. T. (2016). Game theoretical analysis on acceptance of a cloud data access control system based on reputation. *IEEE Transactions on Cloud Computing*, *8*(4), 1003-1017.

[14] Agbaje, M. O., Ohwo, O. B., Ayanwola, T. G., & Olufunmilola, O. (2022). A survey of game-theoretic approach for resource management in cloud computing. *Journal of Computer Networks and Communications*, *2022*.

[15] Yunlong, F., & Jie, L. (2024). Incentive approaches for cloud computing: challenges and solutions. *Journal of Engineering and Applied Science*, *71*(1), 51.

[16] Ding, Y., Li, K., Liu, C., & Li, K. (2021). A potential game theoretic approach to computation offloading strategy optimization in end-edge-cloud computing. *IEEE Transactions on Parallel and Distributed Systems*, *33*(6), 1503-1519.

[17] Chen, Y., Zhao, J., Hu, J., Wan, S., & Huang, J. (2024). Distributed task offloading and resource purchasing

in noma-enabled mobile edge computing: Hierarchical game theoretical approaches. *ACM Transactions on Embedded Computing Systems*, *23*(1), 1-28.

[18] Du, J., Jiang, C., Benslimane, A., Guo, S., & Ren, Y. (2022). SDN-based resource allocation in edge and cloud computing systems: An evolutionary stackelberg differential game approach. *IEEE/ACM Transactions on Networking*, *30*(4), 1613-1628.

[19] Ardagna, D., Panicucci, B., & Passacantando, M. (2011, March). A game theoretic formulation of the service provisioning problem in cloud systems. In *Proceedings of the 20th international conference on World wide web* (pp. 177-186).

[20] Swathy, R., Vinayagasundaram, B., Rajesh, G., Nayyar, A., Abouhawwash, M., & Abu Elsoud, M. (2020). Game theoretical approach for load balancing using SGMLB model in cloud environment. *PloS one*, *15*(4), e0231708.

[21] He, Q., Wang, C., Cui, G., Li, B., Zhou, R., Zhou, Q., ... & Yang, Y. (2021). A game-theoretical approach for mitigating edge DDoS attack. *IEEE Transactions on Dependable and Secure Computing*, *19*(4), 2333-2348.

[22] Kumar, S., Goswami, A., Gupta, R., Singh, S. P., & Lay-Ekuakille, A. (2022). A game-theoretic approach for cost-effective multicast routing in the internet of things. *IEEE Internet of Things Journal*, *9*(18), 18041-18053.

[23] Chi, C., Wang, Y., Tong, X., Siddula, M., & Cai, Z. (2021). Game theory in internet of things: A survey. *IEEE Internet of Things Journal*, *9*(14), 12125-12146.

[24] Abdi, G. H., Sheikhani, A. H. R., Kordrostami, S., Ghane, A., & Babaie, S. (2024). A novel selfish node detection based on reputation and game theory in Internet of Things. *Computing*, *106*(1), 81-107.

[25] Chung, K., Kamhoua, C. A., Kwiat, K. A., Kalbarczyk, Z. T., & Iyer, R. K. (2016, January). Game theory with learning for cyber security monitoring. In *2016 IEEE 17th International Symposium on High Assurance Systems Engineering (HASE)* (pp. 1-8). IEEE.