1. Aim:

To analyze and implement a nash equilibrium-based optimal solution for attacker and defender in cyber-attack scenarios

2.Abstract:

The main objective of the project is to analyze the game's theoretical approach to providing better defense capabilities against an attacker in a cybersecurity environment. A nash equilibrium-based approach is taken to find the best possible action that a defender can take in order to prevent attacks in the system.

3. Keywords:

Nash Equilibrium, Saddle points, Mixed Strategy Nash Equilibrium, Payoff matrix

4. Introduction:

Game theory is a natural approach to modeling the conflict between the attacker and the defender. This work investigates a generalized class of matrix games as a risk mitigation tool to model
these two players in real-world scenarios. In this work, we propose dynamic games
of incomplete information to analyze the interaction between the attacker and defender, where each attacker and defender uses multiple levels of strategy to attack and defend the system's security.
Each player adjusts his strategy based on their strategy costs, potential attack gain or loss, and the effectiveness of the opponent's strategy technique. The payoffs are derived (Original payoff, Expected payoff, Bayesian Nash payoff) and computed (Nash equilibrium, Mixed Nash equilibrium, and Bayesian Nash) to improve the detection rate (maximizing payoffs).

5. Literature:

Recent increases in cyber attacks and identity theft make the Internet seem like a daunting place. Cyber attacks can lead to a severe and rising threat to our society as economic and communication infrastructures heavily depend on computer networks and information technology.

Game theory can answer the question regarding how the defender will react to the attacker, and vice versa, in cyber security. The strategic interaction between them is captured by a two-player game in which each player attempts to maximize his or her interests. The attacker's strategy depends heavily on the defender's actions and vice versa. Thus, the effectiveness of a defense mechanism relies on both the defender's and attacker's strategic behaviors. Using the game-theoretic approach, tactical analysis is performed to investigate the attack from a single node or multiple nodes.

Hence, game theory is useful to investigate the strategic decision-making situations of the defender and/or to analyze the incentives of the attackers.

Game-theoretical approaches overcome traditional solutions to cyber security and network privacy in many aspects, which are described in Table 1:

1	Proven mathematics	Most conventional security solutions, which are implemented either in preventive devices (e.g., firewall) or in reactive devices (e.g., anti-virus programs), rely only on heuristics. However, game theory can methodically investigate security decisions with proven mathematics.
2	Reliable defense	Relying on analytical outcomes from the game, researchers can design defense mechanisms for robust and reliable cyber systems against selfish behaviors (or attacks) by malicious users/nodes.
		While adoption of the traditional security solution is rather slow due

3	Timely action	to the lack of incentives for participants, game-theoretic approaches advocate for defenders by using underlying incentive mechanisms to allocate limited resources to balance perceived risks.
4	Distributed solutions	Most conventional defense mechanisms make decisions in a centralized manner rather than in an individualized (or distributed) manner. In a network security game, the centralized manner is almost an impossible solution due to the lack of a coordinator in an autonomous system. Using appropriate game models, security solutions will be implemented in a distributed manner.

Table 1

The existing works in literature are surveyed in Table 2:

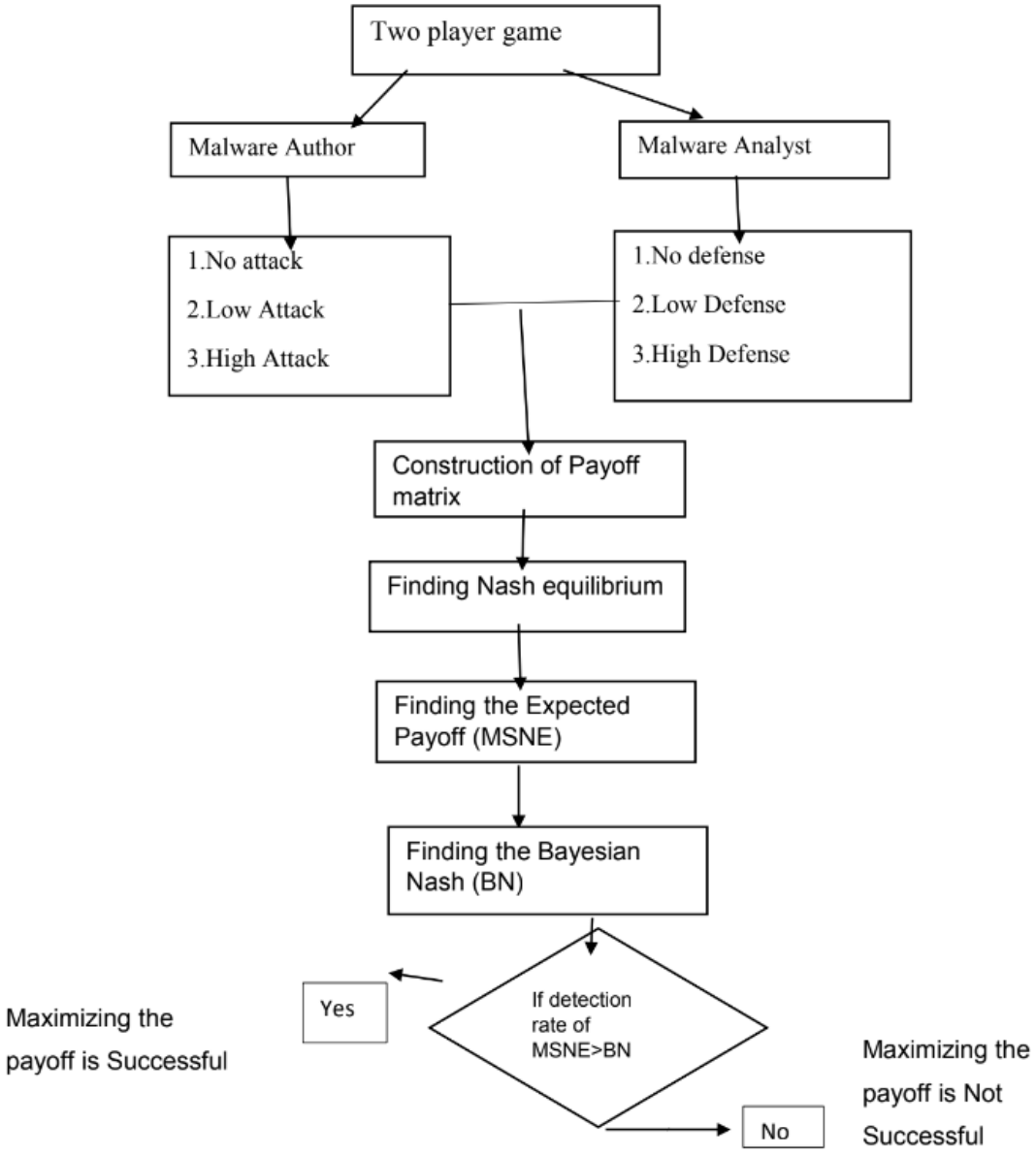
S.No	Authors	Proposed System
1	Chin-Tser Huang, Senior Member, IEEE, Muhammad N. Sakib, Charles A. Kamhoua, Senior Member, IEEE, Kevin A. Kwiat, and Laurent Njilla	In this paper, the Bayesian game model is applied by designing two games to formulate the problem of inspecting Web-based malvertising. The first game has two types of Advertisers, namely Malicious and Benign, and one type of Defender; the second game has two types of Attackers, Advanced, and Simple, in terms of their capability of redirection and evasion, and one type of defender. Their strategies and payoff functions, and compute their Bayesian Nash equilibria.

2	Afraa Attiah, Mainak Chatterjee†, Cliff C. Zou	In this paper, a dynamic game theoretic framework is proposed (i.e., hyper defense) to analyze the interactions between the attacker and the defender as a non-cooperative security game. The key idea is to model attackers/defenders to have multiple levels of attack/defense strategies that differ in effectiveness, strategy, cost, and attack gains/damages.
3	Revan MacQueen, Natalie Bombardieri, James R. Wright, Karim Ali	In this paper, an approach to improve security by modeling attackers and security analysts as a Stackelberg security game is proposed Their method outperforms natural baselines using data from VirusTotal and the National Vulnerability Database.
4	Atin Basuchoudhary, Mohamed Eltoweissy, Mohamed Azab, Laura Razzolini, Shimaa Mohamed	In this paper, cyber defense is modeled as a signaling game. Bayesian Nash equilibria for both the attacker and the defender are found and how these equilibria respond to changes in underlying parameters are characterized.

Table 2

6.Proposed Methodology:

The proposed methodology uses a game theoretic approach to model cyber attack and defense strategies. Classification of action of attacking is split into three categories: level zero, level one, and level two. The attacker can alternate between these three strategies, where level zero represents no attack, level one represents a low-intensity of attack, and level two represents a high-intensity of attack. Likewise, the defender's actions are classified into three corresponding defense strategies. For the proposed security game, there is no Pure Strategy Nash Equilibrium (PSNE) where each player in the game always has the incentive to deviate to another strategy to gain a higher payoff. One can argue that no pair of deterministic strategies work for both players. Therefore, we use mixed strategy nash equilibrium(MSNE) for our model where the opponents become indifferent about the choice of their strategies by making the expected payoffs equal. It is used where attacker-defender face decision-making uncertainty and needs to make decisions based on probabilities. To maximize the payoff of attackers and defenders, we construct the payoff matrix from the dataset values and perform MSNE on each instance of the dataset to calculate the objective function and the optimal distribution of strategies i.e, the probability of each player choosing the maximin strategy where the objective function value represents the maximum of minimum payoff for each player.



Flow chart of Game Theoretic Model

7.Observation:

Payoff matrix:

A payoff matrix is a way to express the result of players' choices in a game. A payoff matrix does not express the structure of a game, such as if players take turns taking actions or a player has to choose without knowing what choice the other will make. Here a payoff matrix for a game between two players is taken, where each player can take three actions: Attacker can take three actions - No Attack, Low Attack, and High Attack and Defender can take three actions - No Defense, Low Defense, and High Defense.

Every combination of choices from Attacker and Defender produces an outcome in the grid. Payoff matrices can be used to model a wide range of scenarios, from simple games to complex decision-making scenarios in business, economics, and politics. They can also be used to model cooperative and non-cooperative games, as well as games with multiple players.

It is observed that the following variables α, β, g, l, Cm1, Cm2, Ci1, and ci2 are needed for calculating the payoff matrix.

The effort and cost employed by the players for performing their intended activities are given as

Cm1 = Cost of launching Low Attack

Cm2 = Cost of launching High Attack

Ci1 = Cost of launching Low Inspection

Ci2 = Cost of launching High Inspection

Upon the success of an attack even in the presence of some measures by the defender:

g = Gain for the attacker

l= Loss incurred for the defender

Probability parameters:

α= Probability of deploying Low Defense by the defender

β= Probability of deploying High Defense by the defender

The following formulas are used for calculating the payoff matrix:

Attacker \ Defender	*NoDefense*	*LowDefense*	*HighDefense*	
NoAttack	$(0, 0)$	$(0, -Ci1)$	$(0, -Ci2)$	$Pa0$
LowAttack	$(-Cm1 + gain, -loss)$	$(-Cm1 + (1-\alpha) * gain),$ $(-Ci1 - (1-\alpha) * loss)$	$(-Cm1 + (1-\beta) * gain)$, $(-Ci2 - (1-\beta) * loss)$	$Pa1$
HighAttack	$(-Cm2 + gain, -loss)$	$(-Cm2 + (1-\alpha) * gain)$, $(-Ci1 - (1-\alpha) * loss)$	$(-Cm2 + (1-\beta) * gain)$, $(-Ci2 - (1-\beta) * loss)$	$1 - Pa0 - Pa1$
	$Pd0$	$Pd1$	$1 - Pd0 - Pd1$	

The game involves a randomized choice of strategies between the attacker and defender, based on the MSNE probability. The probabilities of the attacker choosing No Attack, Low Attack, and High Attack are denoted by Pa0, Pa1, and 1-Pa0-Pa1 respectively, while the probabilities of the defender choosing No Defense, Low Defense, and High Defense are denoted by Pd0, Pd1, and 1-Pd0-Pd1 respectively.

Certain constraints must be adhered to in the game. The cost of launching a High Attack is greater than the cost of launching a Low Attack, which is denoted by Cm2 > Cm1. The gain from launching a Low Attack is greater than the cost of launching a Low Attack, which is denoted by g > Cm1. The gain from launching a High Attack is also greater than the cost of launching a High Attack, which is denoted by g > Cm2. Additionally, g > Cm1 > Cm2.

The defender also incurs a cost for inspecting the attack, and this cost is denoted by Ci1 for Low Inspection and Ci2 for High Inspection. The loss incurred by the defender from an attack is denoted by l, and l > Ci1 and l > Ci2. Additionally, l > Ci1 > Ci2

When the defender plays NO DEFENSE, we compare the attacker's payoff for

- playing **No attack** which is **0**,
- playing **Low attack** which is **–cm1+gain.**
  If –cm1+gain>0 - Low attack is the dominant strategy to No defense and
- playing **High attack** which is **–cm2+gain**.

If –cm2+gain>0 - the high attack can also be the dominant strategy to No defense but with more expense.

When the defender plays LOW DEFENSE, we compare the attacker payoff for

- **No attack** which is **0**,
- playing **Low attack** –cm1+(1-α)*gain–cm2+(1-α)*gain

If **–cm1+(1-α)*gain>0, –cm2+(1-α)*gain>0** then low attack and high attack is the best response to low defense.

If **–cm1+(1-α)*gain<0, –cm2+(1-α)*gain<0** then no attack is the best response to low defense.

When the defender plays HIGH DEFENSE we compare the attacker's payoff for

No attack which is 0
playing **Low Attack** –cm1+(1-β)*gain,–cm2+(1-α)*gain,
If–cm1+(1-β)*gain>0, –cm2+(1-β)*gain>0
then low attack and high attack is the best response to low defense.

If –cm1+(1-β)*gain<0, –cm2+(1-β)*gain<0
then no attack is the best response to low defense.

To determine the best response of the defender to each of the attacker's possible strategies (No Attack, Low Attack, and High Attack), we analyze the payoff matrix.

In the first row, where the attacker plays No Attack, the defender's payoff for playing No Defense is 0, while the payoff for playing Low Defense is -Ci1. Since the cost of Low Inspection and High Inspection must be positive, -Ci1 < 0, and Low Defense is the dominant strategy for the defender against the attacker's No Attack strategy. Similarly, High Defense is the dominant strategy for the defender against the attacker's No Attack strategy if -Ci1 < 0.

In the second row, where the attacker plays Low Attack, the defender's payoff for playing No Defense is -loss, while the payoff for playing Low Defense is (Ci1 - (1-α)loss), and the payoff for playing High Defense is (Ci2 - (1-β)loss). If (Ci1 - (1-α)loss) - (-loss) = -Ci1 + αloss >= 0, then Low Defense is the best response for the defender against Low Attack. If -Ci1 + αloss <= 0, then High Defense is the best response for the defender against Low Attack. Similarly, if (Ci2 - (1-β)loss) - (-loss) = -Ci2 + βloss >= 0, then Low Defense is the best response for the defender to deploy High Defense probability against Low Attack. If -Ci2 + βloss <= 0, then High Defense is the best response for the defender to deploy High Defense probability against Low Attack.

8. Visualizations:

	No defense	Low Defense	High Defense
No Attack	[0, 0]	[0, -0.23]	[0, 0.32]
Low Attack	[0.1, -0.55]	[0.05400000000000002, -0.67]	[0.031, -0.7050000000000001]
High Attack	[0.09, -0.55]	[0.04400000000000001, -0.67]	[0.02099999999999999, -0.615]

Fig.1 Payoff matrix for a dataset instance

```
3
MSNE are : { (0.6361312694295141, 0.36386873057048574, 0.0) , (0.36386873057048547, 0.6361312694295146) }
MSNE are : { (0.6014908608954034, 0.0, 0.3985091391045966) , (0.830267833769992, 0.16973216623000797) }
MSNE are : { (0.7060726795096823, 0.0, 0.29392732049031767) , (0.7140192853172419, 0.28598071468275815) }
```

Fig.2 Objective function and optimal distribution of strategies of the same dataset instance calculated using MSNE

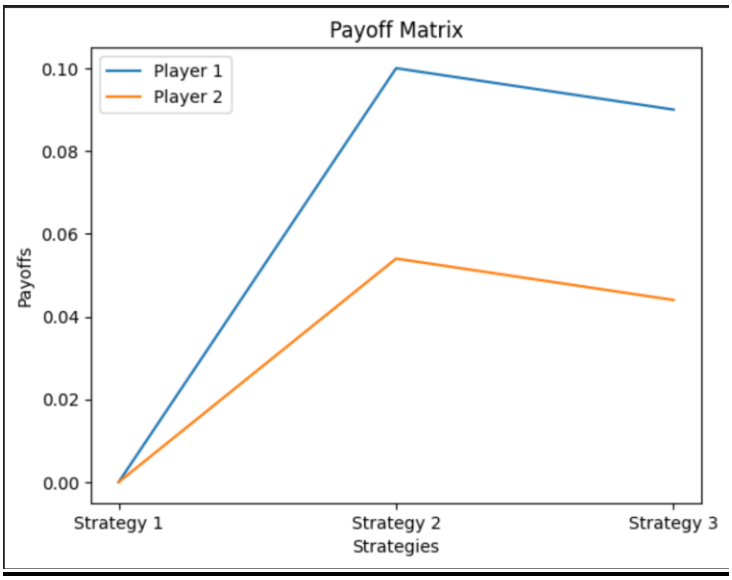


Fig.3 Payoff matrix graph

9. Result:

Thus, the game's theoretical approach to cyber security threats and attacks using nash equilibrium was explored and the payoff matrix and nash equilibrium were successfully calculated for a given dataset.

10. References:

1) A Bayesian Game Theoretic Approach for Inspecting Web-Based Malvertising https://ieeexplore.ieee.org/document/8444673

2) A Game Theoretic Approach to Model Cyber Attack and Defense Strategies
https://ieeexplore.ieee.org/document/8422719

3) Game-Theoretic Malware Detection
https://arxiv.org/abs/2012.00817

4) Game Theory (Normal-form game) | Set 3 (Game with Mixed Strategy)
https://www.geeksforgeeks.org/game-theory-normal-form-game-set-3-game-with-mixed-strategy/?ref=rp

5) Aggarwal, P., Maqbool, Z., Grover, A., Pammi, V. C., Singh, S., & Dutt, V. (2015, June). Cyber security: A game-theoretic analysis of defender and attacker strategies in defacing-website games.
https://ieeexplore.ieee.org/document/7166127

6) L.Y. Njilla, N. Pissinou, and K. Makki, "Game theoretic modeling of security and trust relationship in cyberspace
https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.3115

7) Nash Equilibrium
https://www.investopedia.com/terms/n/nash-equilibrium.asp#:~:text=The%20Nash%20equilibrium%20is%20a,the%20decisions%20of%20other%20players.

8) Mixed Strategy Nash Equilibrium
https://saylordotorg.github.io/text_introduction-to-economic-analysis/s17-03-mixed-strategies.html#:~:text=Key%20Takeaways-,A%20mixed%20strategy%20Nash%20equilibrium%20involves%20at%20least%20one%20player,a%20pure%20strategy%20Nash%20equilibrium.

9) A. Bensoussan, M. Kantarcioglu, and S.C. Hoe, "A game-theoretical approach for finding optimal strategies in a botnet defense model,"
https://link.springer.com/chapter/10.1007/978-3-642-17197-0_9

10) Game Theory in Artificial Intelligence
https://towardsdatascience.com/game-theory-in-artificial-intelligence-57a7937e1b88

11) What is Game theory in AI? Nash Equilibrium
https://www.analyticssteps.com/blogs/essence-game-theory-artificial-intelligence-5-types-game-theory-and-nash-equilibrium

12) Cyberdefense When Attackers Mimic Legitimate Users: A Bayesian Approach
https://ieeexplore.ieee.org/document/7301019