International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 10 Oct. 2024, pp: 104-113 www.ijaem.net ISSN: 2395-5252

Game Theory for Insider Threat Detection and Mitigation: A Review

Olajide O. Ogunbodede[1], Olumide S. Adewale[2], Boniface K. Alese[3], Oluyomi K. Akinyokun[4]

[1] *Department of Software Engineering, Federal University of Technology Akure, Nigeria*
[2]*Department of Computer Science, Federal University of Technology Akure, Nigeria*
[3,4]*Department of Cybersecurity, Federal University of Technology Akure, Nigeria*
Corresponding Author: Olajide O. Ogunbodede

Date of Submission: 05-10-2024 Date of Acceptance: 15-10-2024

ABSTRACT: Malicious insiders pose serious threat to organizations, institutions, and governments' critical infrastructure because of their access to confidential data, systems, and resources. This threat, often referred to as the insider threat, is most of the time regarded as a human factor problem-often driven by motivation, opportunity, and capability. As long as the insider problem is treated as a technology problem, the natural recourse for detection and mitigation is to the use of technical and procedural controls. Such an approach is not advisable when confronting strategic human adversaries, since it may fail to account for the dynamic nature of the conflict between the contending parties who happen to be self-interested and intelligent agents. Game theory, with its rich analytical and modelling techniques, offers mathematical tools and procedures that capture the dynamic interplay between the security apparatus of an organization and the malicious insider. This paper presents a literature review of previous works on insider threat detection and mitigation using game theoretic principles.

KEYWORDS: Insider Threat, Game Theory, Nash Equilibrium, Stackelberg Game.

I. INTRODUCTION

Malicious insiders pose serious threat to organizations, institutions, and governments' critical infrastructure. These individuals often are trusted employees given access to confidential data, systems, and resources. These dangers, which can take many different forms, including theft, sabotage, fraud, and espionage, can have disastrous effects on the organization's finances, reputation, and day-to-day operations, and ultimately the confidentiality, integrity, and availability (CIA) of data.

Information security is literally regarded primarily as a people's problem, and not a technical problem [41]. Subsequently, the insider threat is often deemed a human factor problem. Humans are usually not predictable, difficult to manage in the context of information security, and described as the weakest link in the cybersecurity chain [26], [34]. As long as the insider threat is treated as a technology problem, the human aspects of motivation, opportunity, and capability that happen to be the driving force of any malfeasance behaviour will not be accounted for [2], [35]; thus, rendering any security measures ineffective. Irrespective of their effectiveness, the human behaviour in information security cannot thoroughly be resolved by technical and procedural controls, [30]. Although today's cyberspace is overwhelmed by attacks from outside the organizational perimeter (virtual or physical), it is crucial to look at the interior of this perimeter as well [37].

II. DETECTION

Detection of malicious insiders can be tedious to accomplish. Some systems have been proposed to detect insider threat, some of them utilize proactive forensics [4], graph-based analysis [11], honeypots [43] and other methods. A useful tool in the process of insider detection is intrusion detection systems (IDS) [32], as they can detect abnormal actions, packets with illegal content and deviations from normal user behaviour. Another useful technique, used to mitigate the insider threat, is system call analysis [33], command sequences and windows usage events [39].While intrusion detection systems and honeypots are part of the "network-based sensors" family of technologies, the techniques based on human usage patterns, such as system calls analysis, are part of a larger family of

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 10 Oct. 2024, pp: 104-113 www.ijaem.net ISSN: 2395-5252

techniques known as "host-based user profiling."[39].

The modelling-based approaches for insider threat detection can be classified as shown in Figure 1 below. Game theory as a mathematical tool has always featured where human behaviour and rationality have to be taken into consideration for effective decision making and optimal resource allocation.

Figure 1. Types of insider threat models [38]

III. MITIGATION

According to [44] and [13], even though significant research has been observed in insider threat detection in recent years, relatively little progress has been made overall in mitigating insider threats.

Research in malicious insider threats and attacks have various approaches to their mitigation and causes [13]. However, these mitigation approaches can be grouped into two categories: (a) technical mitigation approaches and (b) non-technical mitigation approaches.

Further, technical approaches toward mitigating insider threats can be grouped into two categories: (a) detecting any unauthorized activity and (b) identifying any changes in behaviours that may lead to a malicious insider threat. These two sub-categories are often operated on digital devices or network operation [12]. Intrusion Detection Systems (IDS), Data Loss Prevention (DLP), Security Information and Event Management (SIEM), Access Control Systems (ACS), or honey-tokens come under technical controls designed to prevent attacks from unauthorized individuals outside the perimeter of an organization. However, these technical controls can also play the dual role of a mitigating technique [21]. Notwithstanding, it is pertinent to note that malicious insiders possess authorized access to the information assets. Thus implying they might have full knowledge of the various defensive mechanisms deployed in the organization. As a result, a typical malevolent insider is often very subtle and will reduce the likelihood of detection to the barest minimum.

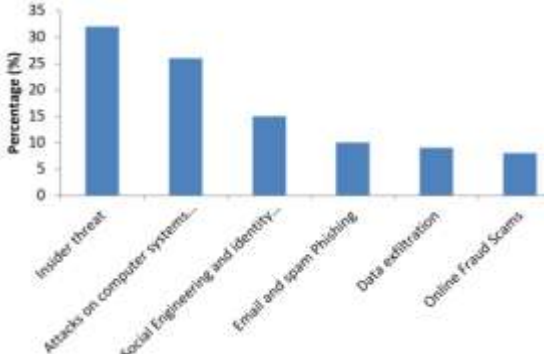

Figure 2. Distribution of the African cost per type cyber-attacks in 2016 [34]

Figure 2 above shows the distribution of the various cyber-attacks cost per type in Africa in the year 2016. Most African enterprises and institutions must have witnessed cases of the malicious insider attack in one form of the other in their existence more than other attacks on computing systems.

IV. GAME THEORY

The control over the computing process and IT systems is actually a cyber-battle between the cybercriminal and the cyber-defender. While the defender continuously invests in resources to maintain full control over his/her computing resources, the attacker on the other hand, continuously strives to wrestle away that control and exercise illegitimate control over those resources [34]. Hence, a new frontier of battlefield that is artificial and highly mutable is opened, called the cyber-battlefield. In this battlefield, cyber-attacks are prosecuted through the use of digital weapons; these weapons are neither limited by geographic boundaries or ideological boundaries. All of the components in the cyber battlefield are human-made. Therefore, it follows that the components and the cyber battlefield may be altered by human beings [17],[34].

Game theory refers to the methodology and framework that uses mathematical tools to model, analyse, and understand interactive decision making processes that often occur among independent, rational, and self-interested agents which could be any of conflict, cooperation, and coordination [27],[31],[34]. These self-interested agents could be: institutions, corporations, software agents, nations, animals etc. Thus, the cyber-battle between the defender (administrator) and the attacker (malicious insider) can be likened to a game with two self-

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 10 Oct. 2024, pp: 104-113 www.ijaem.net ISSN: 2395-5252

interested agents having conflicting vested interests. The ultimate goal of game theory is equilibria: situations in which no participant would relinquish his strategy, if no one else does it as he would be disadvantaged. The first application of game theoretic approaches to security was by [5] in the domain of information warfare.

Game theory tries to predict the behavior of the players in strategic settings and sometimes also provides decision makers with suggestions regarding ways in which they can achieve their optimal goals in a competitive environment [46]. According to [6], game theory offers solutions to mathematical questions about the future actions of participants whose rationality is dynamic [6]. It was introduced into the security domain to confront strategic human adversaries by accounting for their actions, and to proffer quantitative insights and solutions in security management [3].

Since insiders often are well accustomed to the security architecture and setup of their enterprises, the balance and equilibrium often shifts in their favour as the attacker as a result of the information asymmetry [7].

In a typical game, there are two players: a defender and an attacker.The defender is always trying to choose an action to minimize the potential damage that an attacker could cause by taking some preventive actions. The attacker's goal is to maximize the damage. In this sense, the zero-sum games is often used: one player's loss is another's gain. Opponents could either take simultaneous or sequential decisions. Games with simultaneous decisions are referred to as normal form games; in these, all players announce their decision at the same time. In contrast, players in sequential games make their decisions over time, perhaps in response to previous decisions by other players. Most commonly, two players will alternate in declaring their decisions, and these are called extensive form.

Figure 3 below shows the trend of research and publications in various game theory models for insider threat research, from the year, 2015. This shows that there has been upward appreciation and growth in research interest in game theory models and its solution concepts to predict the behaviour of self-interested agents in social interactions in cybersecurity and other relevant fields.

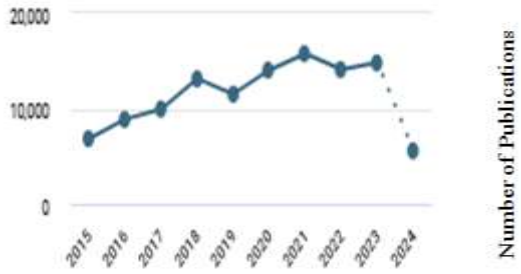

Figure. 3 The trend of security research in game theory for insider threat attacks

V. COMPONENTS OF A GAME

A game is a mathematical model of an interactive decision-making scenario where each player aims to get their optimal result while being aware that every other player is attempting to accomplish the same thing [31].

The essential elements of a game typically are: the players, actions, strategies, payoff functions, and an equilibrium [45].

The players are the individuals, groups, firms, consumers, a government, or non-governmental organizations, or systems that independently make decisions with a bias toward their own self-serving interests and aims. In the context of insider threat mitigation, these are the insiders (employees with access to sensitive information) and the organization (security teams, administrators, and others). Every entity is considered to be rational, with the ultimate goal of maximizing his utility. In this context, utility refers to the degree of contentment, satisfaction, or enjoyment that results from a behaviour. While utility theory is the predominant method for simulating an agent's interests. This theoretical method shows how an agent's preferences vary when he is uncertain about which of the various alternatives he will receive. It also quantifies the agent's degree of preference across the set of alternatives [27]. A utility function is specifically a mapping from real numbers to states of the world. These figures are regarded as indicators of the degree of happiness experienced by an agent in the specified states.

Actions refer to the decisions made each player and it is assumed that each player is fully informed about the options available to them, and the actions that other players may choose to take.

Strategy is a comprehensive contingency plan that details the course of action a player takes in each potential scenario (contingency) that arises throughout the game. In the context of insider threat detection and mitigation, an insider may decide to engage in malicious activities (commit to theft,

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 10 Oct. 2024, pp: 104-113 www.ijaem.net ISSN: 2395-5252

information sabotage, or data exfiltration) or simply comply with organizational policies. On the other hand, the organization may put in place various security measures such as monitoring, access controls, auditing logs to deter or detect insider threats.

Payoff refers to the concept that describes or quantifies the satisfaction that a player derives from under each possible strategy. At the end of each game, the payoff is often made known. The payoff function maps each strategy profile into a real number. For an insider, the payoff could be monetary gain or personal aggrandizement from successful breach of organizational security. The organizational payoffs would be retaining the triad of Confidentiality, Integrity, Availability (CIA), thus retaining trust of clients.

Equilibrium is a collection of mixed strategies (a collection of randomized pure strategies), one for each player. In this scenario, a player will stick to his original plan after considering the opponent's approach and has no reason to change it. In the 1950s, John Nash postulated the Nash equilibrium and deduced that every normal-form game has an associated Nash equilibrium [18]. In non-cooperative game theory, the Nash equilibrium is the most commonly used solution concept.

Games can be classified into different categories based on perspectives. Table 1 shows the classification of games and the security concerns which are related to each classification. Typical games are often classified into either cooperative or non-cooperative. Cooperative game theory is concerned primarily with coalitions or groups of players who coordinate their actions, and pool their winnings [15].

Table 1: Game Theoretic Methods for Cyber Security [36]

Game Models			Application and Security Issues
Cooperative game models	Static game models		mobile ad hoc networks security
Non cooperative game models	Static game models		intrusion detection
			security investment optimization
	Dynamic game models	Complete information game models	security investment optimization
			security incentive mechanism
		Incomplete information game models	cyber attack defence analysis

However, non-cooperative games are the most widely encountered in social settings where competition and diverse interest by the players have to be predicted and resolved. Innon-cooperative game theory, every player or participant tries to maximize his/her own reward regardless of the actions taken by its competitors. Games may be zero-sum or non-zero-sum. In a zero-sum game, every loss by one player is a gain for the other (e.g., as in gambling). In a non-zero sum game, the total gains or losses may be more or less than zero. Nonzero-sum games allow the possibility of win-win solutions among some or all the players (e.g., competing companies might collaborate to develop a product that creates new revenue for both).

VI. REPRESENTING GAMES

The simplest form of representation of a game is a normal-form game. It is regarded as the best-known representation scheme for games (also referred to as the strategic form, or, the bi-matrix form, in the case of two players).

A normal form game G can be represented by a tuple (N, S, u), where
Players: $N = \{1, \dots, n\}$, with typical $i = N$;
Strategies: For every player i, a finite set of strategies, S_i, with typical strategy $s_i = S_i$;
Payoffs: A function $s_i : (s_1, \dots, s_n) \rightarrow \mathbb{R}$ mapping strategy profiles to a payoff for each player $i.u: S \rightarrow \mathbb{R}^n$.
Thus a normal form game is represented by the triplet:

$$G = \langle N, \{S_i\}_{i \in N}, \{u_i\}_{i \in N} \rangle \#$$

Thus, given a strategic form game

$$G = \langle N, \{S_i\}_{i \in N}, \{u_i\}_{i \in N} \rangle, \quad (1)$$

the strategy profile $s^* = (s_1^*, s_2^*, \dots, s_n^*)$ is said to be a pure strategy Nash equilibrium of G if,

$$u_i(s_i^*, s_{-i}^*) \geq u_i(s_i, s_{-i}^*) \; \forall s_i \in S_i, \forall i = 1,2, \dots, n \; \#(2)$$

Where $s_{-i}^*$where denotes s_{-i}^* the profile of actions of all players except N_i

At s^*, no i regrets playing s_i^*. Given all the other players' actions, i could not have done better. That is, each player's Nash equilibrium strategy is an optimal reaction to the other players' Nash equilibrium plans. Every game model takes into account a concept of a solution that establishes the game's result and the strategies that go along with it. Nash equilibrium (NE) is the most famous concept of game solution.

A Nash Equilibrium is a set of strategies of the game under which no single player is willing to unilaterally change his strategy if the strategies of

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 10 Oct. 2024, pp: 104-113 www.ijaem.net ISSN: 2395-5252

the other players are kept fixed. Formally, the action profile $s^* = (s_1^*, s_2^*, \dots, s_N^*)$ is a Nash equilibrium as earlier stated in equation two above. That is, an action profiles$s^* = (s_1^*, s_2^*, \dots, s_N^*)$ is a Nash equilibrium only for each player, the action s_1^* is a best response to the action profile s_{-1}^*.

We refer to an equilibrium strategy as pure strategy equilibrium if it specifies a specific course of action for every actor. There aren't always pure strategy equilibria. However, randomizing the choices made for the actions on the action sets can always result in an equilibrium for a finite, two-player game[18]. Such equilibrium is called a mixed strategy equilibrium. Formally,a mixed strategy selects a probability distribution on the set of actions, whereas a pure strategy selects a deterministic course of action. A mixed strategy of a player is a probability distribution over the set of his or her pure strategies.
If player i has strategies $S_i = \{s_{i1}, s_{i2}, \dots, s_{ik}\}$, then a mixed strategy σ_i for player i is a function on S_i such that $0 \leq \sigma_i(s_{ij}) \leq 1$ and

$$\sigma_i(s_{i1}) + \sigma_i(s_{i2}) + \cdots + \sigma_i(s_{ik}) = 1 \ \#(3)$$

Thus the set of mixed strategies is:

$$\Delta(S_i) = \left\{ x_i \in \mathbb{R}_+^{|S_i|} : \sum_{h \in S_i} x_{ih} = 1 \right\} \#(4)$$

The usual approach of representing games is often through an n-dimensional matrix as shown in figure one, below. The two players are Player 1 and Player 2 with the option of two Strategies A and B each. Player 1 is the row player, while Player 2 is the column player. For example, the pair, p_{1A}, p_{2A} represents the payoff function pairs for each player respectively when Player 1 plays Strategy A and Player 2 plays Strategy B.

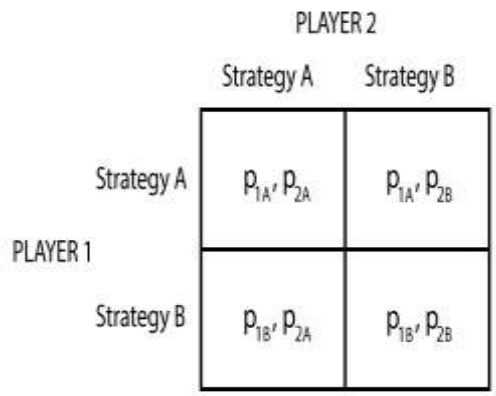

Figure 4. Representing Games with a Matrix

For the pay-off matrix in Figure 1 above, Player 1 is the maximizing player, while Player 2 is the minimizing player. The pay-off values in each row of the matrix is the gain of Player 1, the pay-off values in each column is the loss of Player 2. In the maxmin theorem, the maximizing player, Player 1 lists his worst possible pay offs of all his strategies and chooses that strategies which corresponds to the best. The minimax theorem demands also for the minimizing player, Player 1 to list all his maximum losses from each strategy and select that strategy which corresponds to the least.

A saddle point occurs when the value of the maxmin equals the value of the minimax, and this is called the value of the game.
A maxmin strategy for agent i, strategy σ_i that makes i′s worst case expected utility as high as possible is:

$$\arg\max_{\sigma_i} \min_{\sigma_{-i}} u_i(\sigma_i, \sigma_{-i}) \quad (5)$$

And the maxmin value for agent i, or security level, is the maxmin strategy's worst case expected utility denoted as:

$$\max_{\sigma_i} \min_{\sigma_{-i}} u_i(\sigma_i, \sigma_{-i}) \quad (6)$$

Similarly, the minmax strategy for agent i, strategy σ_i, against agent $-i$ that minimizes the expected utility of $-i$ best response to $\sigma_i$is:

$$\arg\min_{\sigma_i} \max_{\sigma_{-i}} u_{-i}(\sigma_i, \sigma_{-i}) \quad (7)$$

And the agent $-i$ minmax value is $-i$′s maximum expected utility, if agent i plays his/her minimax strategy:

$$\min_{\sigma_i} \max_{\sigma_{-i}} u_{-i}(\sigma_i, \sigma_{-i}) \quad (8)$$

VII. INFORMATION SECURITY AS A GAME

From a game theoretic viewpoint, information security can be compared to a multiplayer game in which there are two teams of players: the attackers, who are malevolent users, and the defenders, who are network/system administrators. There are many advantages to utilizing a game-theoretic method to quantify information security. Above all, it could assist defenders in determining which defense tactics are best for a given system and in estimating the potential loss of those tactics[10],[16].

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 10 Oct. 2024, pp: 104-113 www.ijaem.net ISSN: 2395-5252

In the context of insider threat research, the players include: insiders (with access to sensitive information), the organization (security teams, management, and other employees), and external adversaries (hackers and competitors). The strategies for the insider could to be to act honestly or engage in malicious activities (theft, sabotage, data exfiltration). On the other hand, the defender, the organization can implement various security measures (access controls, auditing, monitoring, training, awareness) as its strategies to deter or detect insider threats [40]. In addition, game theoretic components such as payoffs and information asymmetry are relevant for consideration. For the insider, his payoff could be monetary gain or personal gratification derived from successful malicious acts. The defender's payoff could be successful prevention of security breaches, maintaining trust, and the costs that goes with implementing mitigation strategies. The advantage of information asymmetry is skewed toward the insider in that his intentions are shielded from the organization [22]. Also, his knowledge of the vulnerabilities of the organization favors him compared to the security team. Thus this information asymmetry could play a determining factor in strategy formulation.

VIII. STACKELBERG GAMES

The Stackelberg game is non-symmetric game and a variant of the normal form game where one player observes the move of other player's action before deciding on his/her own action. It is often a sequential, one-shot, finite-action, two-player game [9]. Named after the German economist Heinrich von Stackelberg, who introduced it the early twentieth century, these games illustrate strategic interactions in situations where players make decisions sequentially rather than simultaneously. The first decision maker is the leader, while the second who observes the leader's choice and then chooses its strategy in return, is known as the follower. This sequential nature of decision-making creates a hierarchy in the strategic interaction, where the leader can potentially gain a first-mover advantage by committing to a strategy that the follower must take into account, for example in telecommunications and computational systems for supporting administrative decisions [46]. Stackelberg game has been applied in insider threat research, where the defender sets up its defensive configuration, then an insider discloses the information to the attacker, who can choose to accept or decline it before launching an attack.

IX. REVIEW OF RELATED LITERATURE

Since game theory is widely accepted as an optimization method that models and manages risks from intelligent adversaries [1], [24], and with its rich mathematical principles, it can be effectively applied to identify and mitigate insider threats in organizations by modeling interactions between employees and the organization to predict malicious behavior [42].

This section provides a review of game theory in insider threat mitigation. [29] proposed an insider prediction model for insider threat identification based on a game-theoretic model. This game, they claimed, would assist organizations to understand better malicious insiders' motivations and decision-making processes, thus prescribing the optimal defense strategy. Subsequently, [28] further elaborate on the need to understand inadvertent insider threats through game theoretic analysis of the budget mechanism risk, thus proposing a structured mechanism to mitigate these risks, and evaluating its effectiveness to enhance organizational security. [22] applied game theory to model the interactions between insiders and the security mechanisms, specifically an Intrusion Detection System (IDS), thus gaining further insights into attackers' behaviors.

Further, [23] objective in their paper is to develop a game-based intrusion detection mechanism that specifically targets internal attackers. The authors apply game theory to model the interactions between insiders and the security mechanisms, specifically an Intrusion Detection System (IDS). This approach allows for a structured analysis of the strategic decisions made by both parties involved in the security scenario. [26] proposed a game-theoretic approach for the mitigation of insider threats through a two-player stochastic game that focused on secure team selection and the dynamics between a project manager and an adversary. In this game, a project manager tries to mitigate the likelihood of bribery of a team member to disclose vital information.[25] explore the use of game theory as a new framework to analyze insider threats in the context of nuclear facilities. They contend that their framework is intended to capture the intentions and strategies of both parties, providing a more realistic representation of security dynamics.

[14] proposed the first three-player game model that incorporates the interactions between an attacker, a defender, and an insider as a three-stage Stackelberg game. This model helps in understanding the dynamics between the trio of attackers, defenders, and insiders. Similarly, [14]

explore the complex interactions among the trio of advanced persistent threats (APTs), insiders, and defenders in the context of an enterprise. A non-zero sum game theoretic model with asymmetric feedback is used where the attacker receives delayed feedback regarding the defender's security updates. The paper sheds light on how information asymmetry affects decision-making and strategy formulation for both the attacker and insider.

Furthermore, [8] propose the objective of exploring and establishing a game-theoretical framework that addresses advanced persistent threat (APT) problems, specifically focusing on two types of insider threats: malicious and inadvertent. Subsequently, the paper aims to determine the optimal defense strategies for dealing with both malicious and inadvertent insider threats. This involves analyzing how different types of insider threats affect the defender's approach to security and resource allocation. [7] explores the concept of information asymmetry between defenders and attackers in a three-player game model. The paper highlighted the role private information can play in the effectiveness of security strategies. [20] proposes a novel approach of adversarial risk analysis to insider threat modeling by relaxing the common knowledge assumption of game theory in most models of the threat. In addition, they seek to improve on these models by incorporating additional factors that influence insider threats, such as organizational culture and detection mechanisms.

[19] propose a game-theoretic framework known as the duplicity game that is designed to facilitate the design of deception mechanisms that can effectively counter sophisticated cyber threats as well as mitigate insider threats. Moving further, [42] proposes a game-theoretic modelling approach to capture the interaction between employees and organization to predict malicious employees (insiders) and organizations behavior with incomplete information. This author considers important elements of security culture, elements pertaining to organizational behavior and security as well as game parameters to capture the interaction between employees and organizations.

X. CONCLUSION

In this review paper, we have reviewed several research publications that viewed the insider threat and mitigation from the human factor perspective: strategic actors acting on self-interest. The complexities associated with insider threat make traditional mitigation strategies inadequate. Irrespective of their effectiveness, technical and procedural controls are not sufficient enough to resolve the intricacies and complexities associated with human behavior, and subsequently the insider threat in socio-technical systems. Game theory provides a mathematical framework for analyzing strategic interactions between actors. Thus, game theory models are preferable in strategic settings where the behaviors of self-interested actors have to be taken into consideration and security optimal resource allocations have to be made to minimize the likelihood of adversarial actions.

XI. FUTURE RESEARCH DIRECTIONS

Finally, through this research, we have presented the latest game theoretic frameworks toward mitigating the insider threat. Probable future research directions would be to integrate the human factors of motivation, capability, and opportunity into future frameworks. Also, the Deterrence theory from Situational Crime Prevention perspective can be explored and integrated into future models since most criminal behavior are often carried out with a risk averse tendencies.

REFERENCES

[1]. Anthony, L., & Cox, T. (2009). Game Theory and Risk Analysis. 29(8), 1062–1068. https://doi.org/10.1111/j.1539-6924.2009.01247.x

[2]. Ashenden, D. (2008). Information Security management: A human challenge? Information Security Technical Report, 13(4), 195–201. https://doi.org/10.1016/j.istr.2008.10.006

[3]. Bier, V., Cox, L., & Azaiez, N. (2014). Game Theoretic Risk Analysis of Security Threats. In Igarss 2014 (Issue 1). This is a book with multiple papers

[4]. Bradford, P., & Hu, N. (2005). A Layered Approach to Insider Threat Detection and Proactive Forensics. Proceedings of the Twenty-First Annual Computer Security Applications Conference (Technology Blitz), January 2005. http://www.secretservice.gov/ntac/its

[5]. Burke, D. A. (1999). Towards a Game Theory Model of Information Warfare | Enhanced Reader.

[6]. Camerer, C. F. (2003). Behavioural studies of strategic thinking in games. Trends in Cognitive Sciences, 7(5), 225–231. https://doi.org/10.1016/S1364-6613(03)00094-9

[7]. Cansever, D. (2020). Security Games with Insider Threats. Gamesec-Conf.Org, 1–4.

[8]. Chen, Z., Chen, G., & Hong, Y. (2024). Defense for Advanced Persistent Threat with Inadvertent and Malicious Insider

Threats. Unmanned Systems, 12(2), 341–358. https://doi.org/10.1142/S2301385024410152

[9]. Collins, B., Xu, S., & Brown, P. N. (2024). SoK: Game-Theoretic Cybersecurity: Assumptions, Models, Gaps, and Bridges.

[10]. Do, C. T., Tran, N. H., Hong, C., Kamhoua, C. A., Kwiat, K. A., Blasch, E., Ren, S., Pissinou, N., & Iyengar, S. S. (2017). Game theory for cyber security and privacy. ACM Computing Surveys, 50(2), 30–37. https://doi.org/10.1145/3057268

[11]. Eberle, W., & Holder, L. (2009). Insider threat detection using graph-based approaches. Proceedings - Cybersecurity Applications and Technology Conference for Homeland Security, CATCH 2009, April 2009, 237–241. https://doi.org/10.1109/CATCH.2009.7

[12]. Elmrabit, N., Yang, S. H., & Yang, L. (2015). Insider threats in information security categories and approaches. 2015 21st International Conference on Automation and Computing: Automation, Computing and Manufacturing for New Economic Growth, ICAC 2015, September. https://doi.org/10.1109/IConAC.2015.7313979

[13]. Elmrabit, N., Yang, S. H., Yang, L., & Zhou, H. (2020). Insider Threat Risk Prediction based on Bayesian Network. Computers and Security, 96. https://doi.org/10.1016/j.cose.2020.101908

[14]. Feng, X., Zheng, Z., Hu, P., Cansever, D., & Mohapatra, P. (2015). Stealthy attacks meets insider threats: A three-player game model. Proceedings - IEEE Military Communications Conference MILCOM, 2015-Decem(November 2016), 25–30. https://doi.org/10.1109/MILCOM.2015.7357413

[15]. Fielder, A. (2022). Game theory. In Mathematics in Cyber Research. https://doi.org/10.1201/9780429354649-11

[16]. Ge, H., Zhao, L., Yue, D., Xie, X., Xie, L., Gorbachev, S., Korovin, I., & Ge, Y. (2024). A game theory based optimal allocation strategy for defense resources of smart grid under cyber-attack. Information Sciences, 652, 119759. https://doi.org/10.1016/J.INS.2023.119759

[17]. Ghosh, S., & Turrini, E. (2010). Cybercrimes: A Multidisciplinary Analysis (P. S. Ghosh & T. Elliot (eds.)). Springer Heidelberg Dordrecht London New York. DOI 10.1007/978-3-642-13547-7

[18]. Holt, C. A., & Roth, A. E. (2004). The Nash equilibrium: A perspective. Proceedings of the National Academy of Sciences of the United States of America, 101(12), 3999–4002. https://doi.org/10.1073/pnas.0308738101

[19]. Huang, L., & Zhu, Q. (2021). Duplicity Games for Deception Design with an Application to Insider Threat Mitigation. IEEE Transactions on Information Forensics and Security, 16, 4843–4856. https://doi.org/10.1109/TIFS.2021.3118886

[20]. Joshi, C., Aliaga, J. R., & Insua, D. R. (2021). Insider Threat Modeling: An Adversarial Risk Analysis Approach. IEEE Transactions on Information Forensics and Security, 16, 1131–1142. https://doi.org/10.1109/TIFS.2020.3029898

[21]. Kandias, M., Virvilis, N., & Gritzalis, D. (2013). The insider threat in cloud computing. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6983 LNCS, 93–103. https://doi.org/10.1007/978-3-642-41476-3_8

[22]. Kantzavelou, I., & Katsikas, S. (2009). Playing games with internal attackers repeatedly. 2009 16th International Conference on Systems, Signals and Image Processing, IWSSIP 2009. https://doi.org/10.1109/IWSSIP.2009.5367708

[23]. Kantzavelou, I., & Katsikas, S. (2010). A game-based intrusion detection mechanism to confront internal attackers. Computers & Security, 29(8), 859–874. https://doi.org/10.1016/J.COSE.2010.06.002

[24]. Kim, K.-N., Suh, Y.-A., Schneider, E., & Yim, M.-S. (2015). Physical Protection System Design Analysis against Insider Threat based on Game Theoretic Modeling. Transactions of the Korean Nuclear Society Spring Meeting Jeju, 8–11.

[25]. Kim, K. N., Young, S., Schneider, E., & Yim, M. S. (2014). A Game Theoretic Approach to Nuclear Security Analysis against Insider Threat. Transactions of the Korean Nuclear Society Spring Meeting.

[26]. Laszka, A., Johnson, B., Schöttle, P., Grossklags, J., & Böhme, R. (2013). Managing the weakest link: A game-theoretic approach for the mitigation of

insider threats. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 8134 LNCS(September), 273–290. https://doi.org/10.1007/978-3-642-40203-6_16

[27]. Leyton-Brown, K., & Shoham, Y. (2008). ESSENTIALS OF GAME THEORY. A Concise, Multidisciplinary Introduction.

[28]. Liu, D., Wang, X., & Camp, L. J. (2009). Mitigating inadvertent insider threats with incentives. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 5628 LNCS, 1–16. https://doi.org/10.1007/978-3-642-03549-4_1

[29]. Liu, D., Wang, X. F., & Camp, J. (2008). Game-theoretic modeling and analysis of insider threats. International Journal of Critical Infrastructure Protection, 1, 75–80. https://doi.org/10.1016/J.IJCIP.2008.08.001

[30]. Mahfuth, A. (2019). Human Factor as Insider threat in Organizations. International Journal of Computer Science and Information Security (IJCSIS), 17(12), 42–47. https://sites.google.com/site/ijcsis/

[31]. Maschler, M., Solan, E., & Zamir, S. (2013). Game Theory. In Cambridge University Press (Vol. 39, Issue 2). Cambridge University Press. https://doi.org/10.1176/pn.39.2.0031b

[32]. Mun, H., Han, K., Yeun, C. Y., & Kim, K. (2008). Yet Another Intrusion Detection System against Insider Attacks. Proc. of SCIS2008, 1–6. http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Yet+Another+Intrusion+Detection+System+against+Insider+Attacks#0

[33]. Nguyen, N., Reiher, P., & Kuenning, G. H. (2003). Detecting insider threats by monitoring system call activity. IEEE Systems, Man and Cybernetics Society Information Assurance Workshop, June 2001, 45–52. https://doi.org/10.1109/SMCSIA.2003.1232400

[34]. Ogunbodede, O. O. (2023). Game Theory Classification in Cybersecurity: A Survey. Applied and Computational Engineering, 2(1), 670–678. https://doi.org/10.54254/2755-2721/2/20220644

[35]. Padayachee, K. (2013). A conceptual opportunity-based framework to mitigate the insider threat. 2013 Information Security for South Africa - Proceedings of the ISSA 2013 Conference. https://doi.org/10.1109/ISSA.2013.6641060

[36]. Patil, A. P., & Annigeri, N. M. (2018). Applications of Game Theory for Cyber Security System: A Survey. In International Journal of Applied Engineering Research (Vol. 13). http://www.ripublication.com

[37]. Raut, M., Dhavale, S., Singh, A., & Mehra, A. (2020). Insider threat detection using deep learning: A review. Proceedings of the 3rd International Conference on Intelligent Sustainable Systems, ICISS 2020, 856–863. https://doi.org/10.1109/ICISS49785.2020.9315932

[38]. Raval, M. S., Gandhi, R., & Chaudhary, S. (2018). Insider Threat Detection: Machine Learning Way. In Advances in Information Security (Vol. 72, pp. 19–53). https://doi.org/10.1007/978-3-319-97643-3_2

[39]. Salem, M. Ben, Hershkop, S., & Stolfo, S. J. (2008). A Survey of Insider Attack Detection Research. Advances in Information Security, 39(May), 69–70. https://doi.org/10.1007/978-0-387-77322-3_5

[40]. Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. Electronics (Switzerland), 9(9), 1–29. https://doi.org/10.3390/electronics9091460

[41]. Schultz, E. (2005). The human factor in security. Computers and Security, 24(6), 425–426. https://doi.org/10.1016/j.cose.2005.07.002

[42]. Sepehrzadeh, H. (2022). Predicting Malicious Behavior of Employees using Game Theory. 0–13. http://dx.doi.org/10.21203/rs.3.rs-2258002/v1%0Ahttps://www.researchsquare.com/article/rs-2258002/v1

[43]. Spitzner, L. (2003). Honeypots: Catching the insider threat. Proceedings - Annual Computer Security Applications Conference, ACSAC, 2003-Janua, 170–179.

https://doi.org/10.1109/CSAC.2003.1254322

[44]. Walker-Roberts, S., Hammoudeh, M., & Dehghantanha, A. (2018). A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure. IEEE Access, 6(1), 25167–25177. https://doi.org/10.1109/ACCESS.2018.2817560

[45]. Watson, J. (2013). Strategy. In J. Repcheck (Ed.), W.W. Norton & Company. W.W. Norton & Company, Inc., 500 Fifth Avenue, New York, NY 10110-0017.

[46]. Wilczyński, A., Jakóbik, A., & Kołodziej, J. (2016). Stackelberg security games: Models, applications and computational aspects. Journal of Telecommunications and Information Tecfile:///C:/Users/OlajideO Ogunbodede/Desktop/PROJECT-MAIN/LEYTON_BROWN-Yoav Shoham --GAME THEORY.Pdfhnology, 2016(3), 70–79. https://doi.org/10.26636/jtit.2016.3.749