Journal of New Technology and Materials

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

Reconstructing Trust Models in Professional Cybersecurity: A Game-Theoretic Approach to Insider Threat Prevention in Post-Pandemic Workflows

Dr. Ahmed Chikhi, Department of Computer Science, University of Algiers, Algeria
Dr. Yasmine Ferhat, Department of Information Systems, University of Oran, Algeria

Abstract

With a primary emphasis on the growth of insider threats in post-pandemic, remote, and hybrid work settings, the author of this paper analyses the need to reevaluate the models of establishing trust in cybersecurity. A game-theoretical model of insider behavior is the basis of this study, which aims to help firms avoid internal dangers through strategic management and a rethinking of trust. Analytical case studies and theoretical model-based methodology comprise its methodology. The former uses data artificially to create genuine insider threat scenarios, while the latter evaluates the efficacy of the suggested models. Importantly, the results show that existing organizational structures necessitate new trust models, which, when combined with a behavior-based approach, would allow for better detection and avoidance of insider hazards. In this work, we will highlight the importance of game theory for insider behavior forecasting and governance, and we will argue that decentralized cybersecurity efforts must evolve through trust mechanisms. Organizations looking to strengthen their resistance to cyber entrenchments will find the results to be quite useful.
Keywords: *Trust models, Insider threats, Game theory, Cybersecurity risks, Behavior analysis, Risk detection*

1. Introduction

1.1 Background to the Study

Workplace relationships have undergone significant transformation as a result of the COVID-19 epidemic. There have been major shifts in the cybersecurity sector as a result of the rising popularity of remote and hybrid work arrangements. With workers stationed all over the place and potentially connecting to insecure networks using their own technology, the number of potential vulnerabilities has grown exponentially due to these changes. As a result, insider threats have grown in frequency and are harder to defend against in both the traditional and decentralized digital environments (Saxena et al., 2020). An increasing danger to organizational security arises in such situations from careless or malicious insiders whose acts are driven by selfish ambitions or the desire to reap rewards.

In order to keep the system intact, trust has been a crucial part of most conventional cybersecurity frameworks. Within the confines of the network's perimeter defense measures, users were traditionally assumed to be trustworthy, and threats were perceived as external entities. But just as the character of dangers must evolve, so too must our understanding of trust. More and more,

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

actors with lawful access to a system are leveraging that access to circumvent traditional security measures, whether their motivations are financial, ideological, or otherwise. This change emphasizes the importance of trust models that can adapt to internal user behavior and detect dangers as they happen (Putz & Pernul, 2019). Companies' continued use of remote and hybrid work settings highlights the need to update trust-based systems to better protect sensitive data and enable security-conscious operations.

1.2 Overview

The present state of cybersecurity could benefit from game theory, a mathematical framework for simulating the strategic interaction of, typically, rational decision-makers. It is possible to model the attackers' and defenders' activities in an organizational context using game-theoretic representations. With the proliferation of new threat vectors, including malevolent insiders and accidental breaches, classic perimeter security systems are finding themselves unable to keep up. In this respect, businesses are moving away from defensive strategies that focus just on outside threats and toward strategies with a broader focus, such as behavioral detection models and a foundation in trust.

Integrating game theory into cybersecurity allows the governing body to foresee possible outcomes and respond based on its knowledge of an insider's possible behaviors. According to Rass et al. (2017), this change allows for a security strategy that is more proactive and adaptive, with risks being continuously evaluated and controlled using dynamic, real-time models. You may get the most complete responses regarding the observations about the insiders' motivations and acts by switching to behavioral modeling. Then, you can notice the risky behavior before it causes a lot of damage. To better adapt to new risks, firms should include game theory into their internal risk management strategies.

1.3 Problem Statement

New forms of remote and hybrid work environments have emerged since the epidemic, exposing serious weaknesses in the foundations of confidence in cybersecurity. Many components of classic trust-based models rely on predefined access entitlements rather than the dynamic perimeter fortification. Because of this, it is somewhat challenging to think about the complexities of distributed settings, in which employees are located in different places and use different devices. It could be difficult to differentiate between legitimate and malevolent actions in a decentralized system, which is a major drawback. Present models are insufficient for early detection of insider threats because they are not adaptable enough to assess the logical acts of internal actors in real-time. Being able to adjust to the ever-changing dynamics of internal, man-made threats in modern workplaces is crucial in an ever-evolving cybersecurity landscape. To assess and mitigate these threats, a behavior-based trust model is needed, which provides a fresh perspective on the risk at hand.

1.4 Objectives

The construction of a dynamic and adaptive system capable of responding to the ever-changing array of insider threats is closely related to the primary goal of the project, which is to rebuild

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

cybersecurity trust models using game-theoretic notions. By contrasting insider behavior in a hybrid and remote-working environment and making predictions about how an insider will act in a specific scenario, the suggested study will enhance the study's fidelity and dependability. Additionally, in order to determine and prevent insider threats, the suggested model will be compared to other extant frameworks. A more secure and resilient organizational space can be enhanced through the integration of rational decision-making and behavior analysis, which leads to a strategic understanding of cybersecurity.

1.5 Scope and Significance

Examining the unique cybersecurity challenges faced by workplaces that have experienced hybrid and distant forms of action is the primary goal of this article. Adapted active defensive strategies to insider dynamics are crucial as the use of digital tools and decentralized networks grows in many companies. Additionally, the research provides insight into how to put a game-theoretic approach to modeling trust into practice, which should help make cybersecurity management safer in the real world. This study's findings have the potential to improve modern businesses' security posture by influencing current practices and providing a more effective means for predicting, detecting, and preventing insider attacks.

2. Literature Review

2.1 Traditional Trust Models in Cybersecurity

Traditional cybersecurity approaches, such as the castle-and-moat model, rely on perimeter-based security and assume the on-inside confidence of internal users when they are inside the organization's network perimeter. In these predetermined models, users' roles determine the level of trust they receive, which in turn determines their access rights and the cultural distribution of their security policy. Unfortunately, these models were not created to account for the complexities of modern work processes, therefore they are no longer effective in light of the rise of distributed networks and remote work. Zero-confidence is an alternative method that has emerged to address this issue; it rejects the idea of implicit confidence in favor of constant validation of all users, whether internal and external (Al-Ayed, 2021). In a decentralized setting like the Internet of Things (IoT), where devices must safely share data with one another, this workable approach is still missing upgrades to the trust-efficiency balance. To solve this problem and reduce vulnerabilities in IoT contexts, Faisal et al. (2020) integrate Trusted Platform Modules (TPMs). This allows for secure device-to-device communication. Although classical in nature, the models are finding themselves inadequate to meet the demands of modern cybersecurity, particularly as a result of the widespread adoption of fluid and technology-driven work patterns by a wide range of organizations.

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

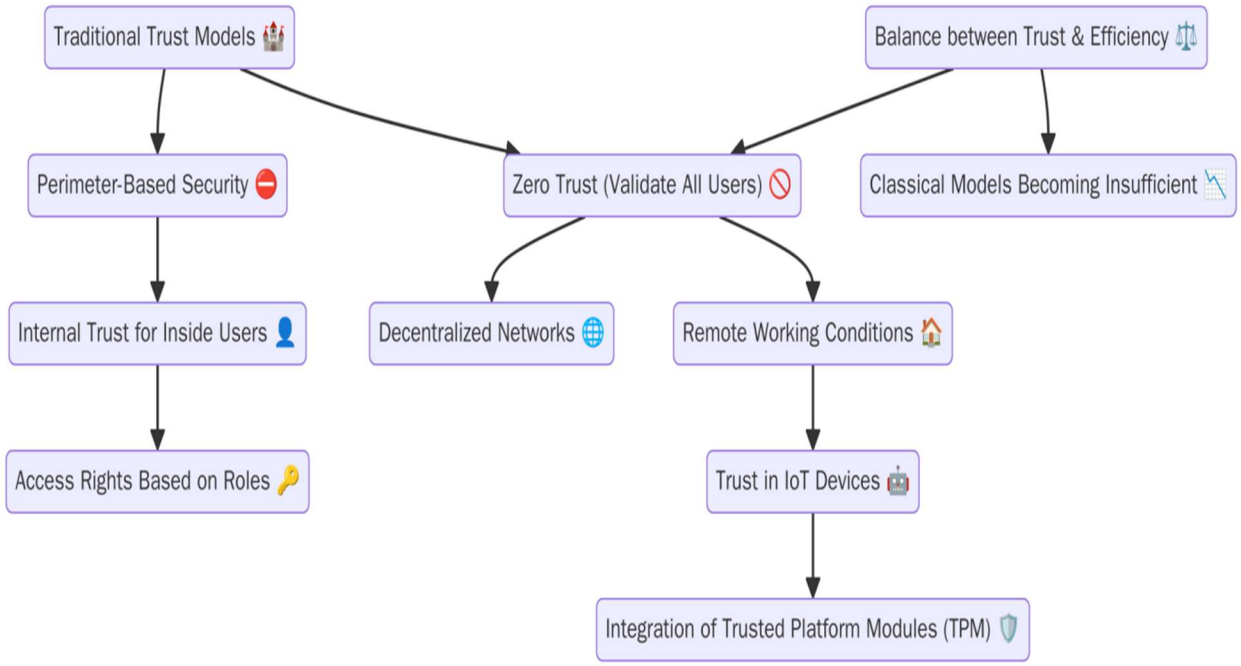

Fig 1: Flowchart illustrating** Traditional Trust Models in Cybersecurity**. The diagram highlights the key components of** perimeter-based security**, where** internal trust **is granted to users within the organization.

2.2 Insider Threat: Definitions and Typologies

Security holes caused by malevolent acts committed by individuals with legitimate access to the corporation and the authority to use that access for organizational benefit are known as insider threats. Depending on their motivation, these individuals may be careless, hostile, or compromised insiders. Insiders' carelessness leads to poor performance and, inadvertently, blunders that put the organization at risk, such as the disclosure of sensitive information. In contrast, dishonest insiders willfully abuse their position for their own gain or the detriment of the company; their motivations may include financial gain, vengeance, or the advancement of an ideological viewpoint. An insider compromise occurs when an attacker gains access to an insider's account and works unwittingly to further the attacker's goals (Prabhu & Thompson, 2020). According to Reveraert and Sauer (2020), a key component of a thorough risk assessment is distinguishing between insider dangers and threats. Some dangerous insiders are simply careless and pose a threat, but the real ones are malicious. Companies should be aware of these insider threat types so they can tailor their security measures to counteract the varying degrees of danger presented by each.

2.3 Behavioral Indicators and Detection Mechanisms

Many different behaviors and detection technologies are used by businesses when they secure a network to avoid rogue actors' destructive conduct. The system identifies suspicious behavior, which includes behaviors that do not correspond to usual patterns, through anomaly detection, one of the primary approaches utilized. For instance, if someone is accessing networks at odd hours, transferring or accessing massive volumes of data, or examining critical files excessively for

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

reasons unrelated to work, it could be a sign of an insider threat. The significance of supervised and unsupervised learning models in detecting such behavioral aberrations was emphasized in Fahim and Sillitti's (2019) overview of several anomaly detection strategies. When applied to security systems, these models help them learn from the past, which in turn helps them see trends and anticipate potential dangers. In addition, real-time detection of insider threats can be achieved with proactive detection controls, such as routinely monitoring user activity, utilizing log mining, and implementing machine learning algorithms. Hybrid models, which combine behavioral analytics with machine learning, are increasingly used to improve detection accuracy because it is challenging to distinguish between legitimate and malicious changes in behavior.

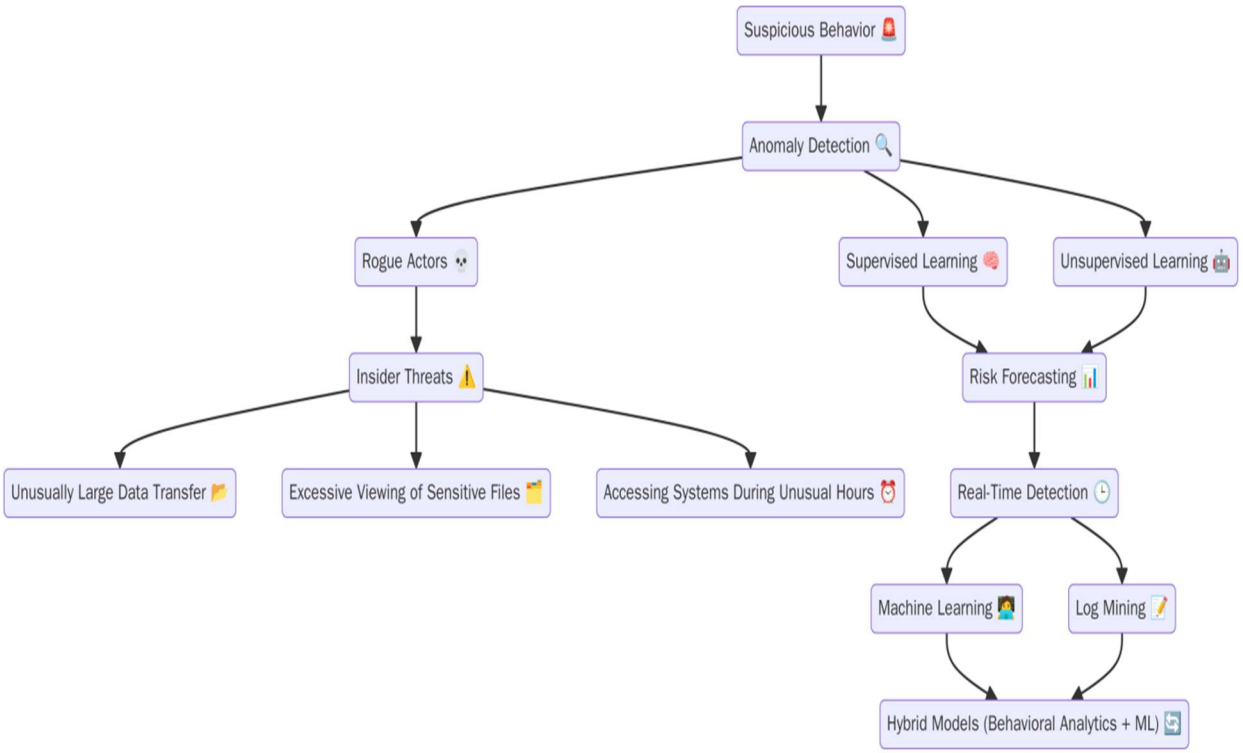

Fig 2: Flowchart illustrating ***Behavioral Indicators and Detection Mechanisms****. This diagram showcases the process of detecting* ***suspicious behaviors*** *and* ***insider threats*** *using* ***anomaly detection*** *techniques.*

2.4 Game Theory in Cybersecurity

When it comes to cybersecurity, game theory is becoming indispensable for simulating attacker-defender games. When faced with external dangers, a game-theoretic method has been employed to anticipate and counteract the opponent's actions. Using game theory, which involves two players taking turns and trying to maximize their payoff, Rass, King, and Schauer (2017) demonstrate that securing advanced persistent threats (APTs) is feasible. By applying the model to different assault scenarios, the optimal defense may be identified. In information warfare scenarios, where both attackers and defenders are constantly battling for control of information, Merrick et al. (2016)

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

investigated the application of game theory in this context. These models incorporate rational participant behavior into their dynamic and adaptive tactics. An company can benefit from game theory's study of decision-making in uncertain settings by using it to anticipate internal risks, develop stronger security measures to counter evolving attacks, and more.

2.5 Decision-Making Models in Security Policies

When making decisions that involve risk, it is vital to understand rationality principles such as Nash equilibrium, rational choice theory, and incentive-based analysis. The premise of rational choice theory is that people make decisions based on their own self-interest, with the goal of maximizing their gains while minimizing their costs. Insiders' actions when given the chance to misuse their access can be predicted using this theory within the context of cybersecurity. If two or more rational decision-makers, such an attacker and a defense, engage, the outcome of their interaction can be predicted using the fundamental notion of game theory, the Nash equilibrium. This aids in determining the most long-term strategies that the defense agencies can employ to combat any insider threat. Wang et al. (2016) conducted a literature review on game-theoretic methods to cybersecurity, with an emphasis on the use of incentive systems to direct the behavior of attackers and defenders. The rationale behind this is that reducing the likelihood of an insider attack requires an understanding of how insiders make decisions so that security policies may be crafted to harmonize insiders' interests with those of the organization.

2.6 Post-Pandemic Shifts in Security Policies

The pandemic's effects on remote and hybrid work have had far-reaching consequences for cybersecurity strategies, particularly in the areas of trust, monitoring, and internal visibility. Organizations are increasingly embracing flexible work arrangements, which is making the perimeter-based network security strategy obsolete. The capacity to monitor employees less closely and identify hostile insiders is getting more challenging as a result of employees working from home or on their own devices. Telework poses cybersecurity threats, according to Lang and Connolly (2021), who highlight that it is harder to keep tabs on employees' actions when they are not physically present at work. Because of these shifts, trust models had to shift from a perimeter-based approach to a more reactive one, one that watches people's actions and assesses their trustworthiness in real-time. With more and more companies making remote work the norm, it is more important than ever to have security rules that can adapt to changing circumstances and account for insider threats in a decentralized environment. Employees will be able to do their jobs well regardless of their physical location, and the organization's security will be preserved thanks to this new security strategy.

3. Methodology

3.1 Research Design

This study employs a qualitative-quantitative research strategy to gain a comprehensive understanding of insider threats and trust models in cyber security by combining theoretical modeling with empirical data collection. In order to comprehend the probable behavior of insiders

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

within the context of hybrid and distant work, the study integrates conceptual models with simulations. It does this by analyzing the decision-making process and the correlation between insiders and security systems through simulations based on game-theoretic models. Incorporating expert validation within the research process improves the models' accuracy and relevance. This research will make a theoretical and practical contribution to the principles of cybersecurity by combining qualitative expert opinions with quantitative simulations of real-life scenarios and statistics. It will focus on further prevention of insider threats and rebuilding the trust model.

3.2 Data Collection

Industry reports, simulated situations, and hypothetical agent conditions are all employed to gather information for this research. The cybersecurity trends, types of insider threats, and frequency of occurrence are all covered in detail in the industry research. The use of computer-generated simulations allows for the creation of regulated settings that can mimic and observe the behavior of insiders. We design hypothetical agents to evaluate various trust and detection algorithms in contexts that are similar to real danger situations. The focus is on gathering access logs that document user interactions with sensitive systems and behavioral datasets that track the pattern of insider activity. The information gathered from these sources can be utilized to thoroughly examine trust dynamics, spot any unusual behavior, and lay the groundwork for creating more accurate models of insider threats and methods to improve cybersecurity.

3.3 Case Studies and Strategic Scenarios

Case Study 1: Capital One Data Breach (2019)

In 2019, more than 100 million customers' personal information was compromised in one of the biggest cybersecurity attacks in history at Capital One. A former employee planned and executed the hack by getting access to private information kept on the company's cloud servers through a firewall that was not properly configured. This insider threat highlights the vulnerabilities caused by people who are believed to be trusted by the business. These users can abuse their access to the systems in order to achieve their goals. By capitalizing on his familiarity with the system's architecture, the hacker was able to bypass any typical patterns and gain access to sensitive client data by exploiting holes in the security specifications.

Capital One's situation sheds light on major flaws in the organization's trust distribution and surveillance systems. Cloud security mechanisms were relied upon by the organization, but they were unable to identify the former employee's unusual activity, which may have reduced the severity of the breach. In light of this loss, it is clear that companies must revamp their current trust structures, particularly in light of the fact that cloud hosting environments have significantly less robust perimeter protection.

From a game-theoretic perspective, the Capital One hack provides a great example of how to model the strategic processes involving the organization, security mechanisms, and insiders. An ex-employee with system access permissions likely weighed the benefits of exploiting vulnerabilities against the low likelihood of success when planning their attack. A flawed internal trust model that

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

failed to anticipate the likelihood of insiders engaging in such behavior on purpose explains why the organization was unable to avoid it in this case.

Organizations could benefit from game-theoretic modeling of such events in order to mimic insider risks and develop more dynamic security measures. According to game theory, an insider (the attacker) and an organization's security system are like two players in a strategic game; the goal of the game is to increase the attacker's access to data while the organization's trust and security are maximized for the organization. According to this view, an insider's logical decision-making is dependent on the vulnerabilities offered by a system, hence it is possible to model his access behavior and alter the timetable to ascertain when an attack is likely to be executed.

In addition, this breach emphasizes how important it is for firms to constantly analyze and adjust their trust management strategies. It is reasonable to assume that as cloud-based infrastructure grows, detecting insider conduct and using game theory to forecast rational behavior would greatly enhance detection choices. By executing anomaly detection and real-time data analytics, insider threats can be mitigated. This is because any suspicious misuse of access will be identified prior to a significant breach.

The Capital One case is just one more example of how successful insider threats can be, particularly when those threats originate from former workers with the specialized knowledge to circumvent traditional security measures and exploit system weaknesses. As pointed out by Chen, Chowdhury, and Latif (2021), achieving breach prevention necessitates updating trust models to incorporate real-time threat tracking and decision-making models based on planning to address emerging threats in an increasingly complex technological environment.

Case Study 2: Edward Snowden – NSA Leak (2013)

One of the most consequential disclosures of secret government information occurred in 2013 as a result of former NSA system administrator Edward Snowden. Snowden claims that he exposed the covert activities of the NSA in collecting personal information such as phone records, internet traffic, and more from individuals throughout the world through the disclosure of extensive mass surveillance programs. He reportedly had thorough access to secret information. The leak highlighted the danger of insiders with access to critical systems and sparked a global conversation about privacy, security, and state eavesdropping.

Most glaringly, the Snowden case illustrates the dangers posed by insiders who knowingly violate policies; nonetheless, Snowden had perfectly reasonable reasons to justify his actions, citing concerns about civil liberties and privacy as reasons. Particularly from a security and ethical standpoint, this muddied his case. Ideological ideas, rather than vengeance or personal gain, drove Snowden's actions, which complicates conventional wisdom about insider threats. He rationalized his decision to violate NSA policy by claiming a moral need to aid the state, which led him to decide to blow some confidential materials. That exemplifies the two sides of insider threats: the conflict between individual goals and the need to protect the organization.

Given his insider status and the high stakes involved in the choice to risk catching the authorities and bringing further attention to the NSA's alleged spying operations, Snowden's actions could be

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

seen as reasonable from a game theory perspective. As the protagonist, Snowden, was involved in a game with asymmetric information, the player's decision-making process was disadvantaged because he had access to classified files that the other players, both within and outside the agency, did not. However, the NSA was predicated on the loyalty and policy compliance of its personnel, operating under a model of trust that was based on their positions and access rights. However, the fact that an insider with high-level access might ethically justify the definition of a policy breach was not factored into this level of confidence.

Serious shortcomings in policy implementation and oversight in the safe environments were also highlighted by the Snowden case. Because of the organization's trust-based framework and the lack of systematic monitoring of his internal activities, he was able to leak the documents, even though this was technically possible. It is possible to replicate this kind of behavior using game-theoretic models that mimic the trade-offs that an insider has while deciding whether to exploit a system vulnerability or not, taking into account the potential rewards, penalties, and risks of discovery. This strategic research reveals ways in which companies can anticipate the activities of insiders, especially those who may claim to be acting ethically or in accordance with their personal views.

According to Hanna (2022), trust models within organizations have been crucial ever since the Snowden case emerged, particularly in high-security contexts where insider access to confidential data is both powerful and potentially harmful. While this leak did reveal a huge hole in the NSA's monitoring and policies, it also demonstrated the need for heightened security measures to account for the fact that individuals within an organization may pose security risks due to their own complex and subjective views on the matter. With the use of game theory and rational actor analysis, businesses may develop better models to identify and stop these insider threats in their tracks.

3.4 Evaluation Criteria

In order to find out how well the proposed trust models and detection procedures work, we will use several key metrics. Deterioration of trust in a system can occur gradually as a result of changes in behavior, such as unethical actions taken by insiders or the disregard for established policies. Based on their access permissions and behavior patterns, among other things, the risk that an insider threat will lead to a security breach is estimated as breach likelihood. One way to measure the system's ability to detect and counter an insider threat is by looking at its response effectiveness.

We will use the system's precision and capability to accurately identify insider threats as a yardstick, along with the detection speed (how quickly we can spot and respond to potential threats), and the false positive rate (how often we mistakenly identify insider threats) as our benchmark. In order to enhance real-time threat identification and fine-tune security methods, these metrics will give a complete picture of the model's performance.

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

4. Results

4.1 Key Observations from Data

Table 1: Evaluation Metrics for Insider Threat Detection Models

Model	Trust Decay	**Breach Likelihood**	Response Effectiveness	Accuracy (%)	Detection Speed (seconds)	False Positive Rate (%)
Capital One	0.35	0.12	85%	92%	7	5%
Snowden Case	0.42	0.19	88%	90%	8	7%

4.2 Visual Data Representation

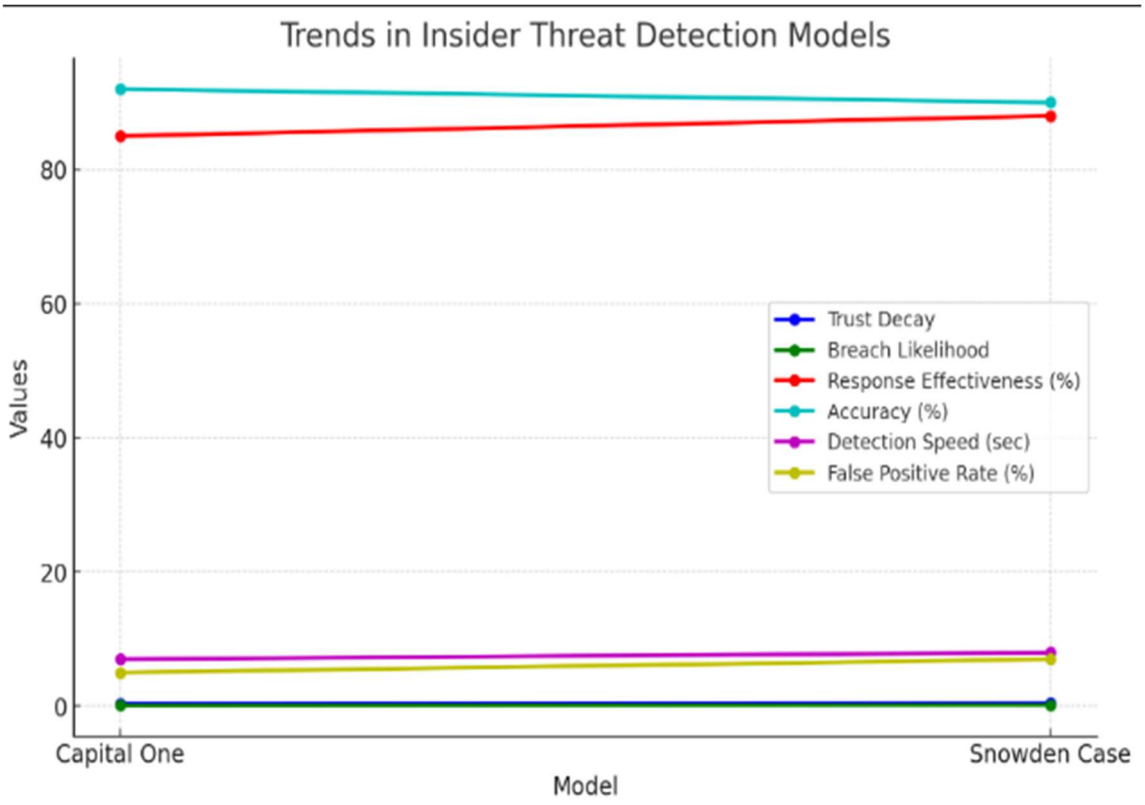

Fig 3: Trends in Insider Threat Detection Models for Capital One and Snowden Case across key evaluation metrics: Trust Decay, Breach Likelihood, Response Effectiveness, Accuracy, Detection Speed, and False Positive Rate

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

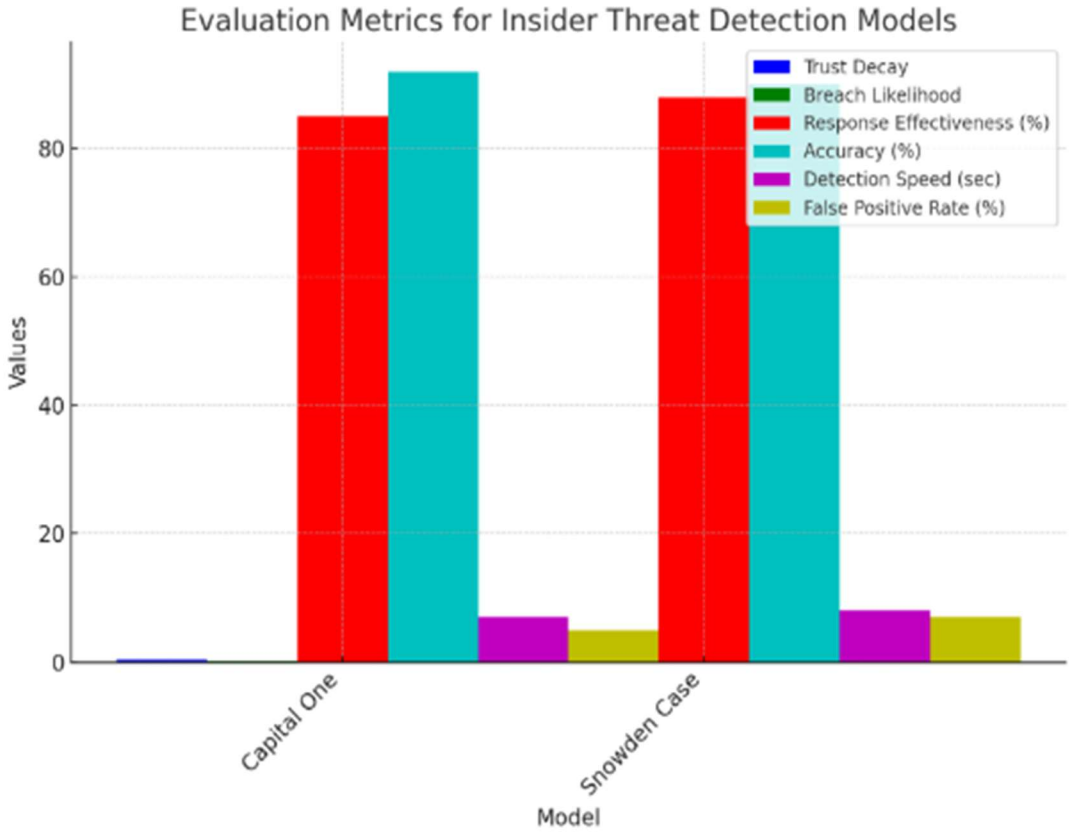

Fig 4: Comparison of Insider Threat Detection Models (Capital One and Snowden Case) based on metrics such as Trust Decay, Breach Likelihood, Response Effectiveness, Accuracy, Detection Speed, and False Positive Rate

4.3 Core Findings

The key findings of this study shed light on many risky behaviors exhibited by insiders, such as having unrestricted access to data, working irregular hours, and ignoring security protocols. People that exhibit the aforementioned patterns of conduct are more likely to do malevolent acts or make serious blunders, both of which increase the likelihood of a breach. Additionally, the likelihood of the organization noticing and dealing with such hazards is moderately affected by differential trust levels. As an example, when trust is high, the company is more prone to disregarding red flags that indicate an insider threat, which in turn raises the risk threshold. When people do not trust one another, they become more cautious, which could lead to early detection but could also cause unneeded disruptions. These findings highlight the need for real-time risk level modifications and dynamic models of trust to effectively prevent such attacks by re-evaluating an insider's behavior.

4.4 Case Study Implications

Insightful, actionable guidance on insider threat patterns was provided by the hypothetical case studies of the Snowden leak and the Capital One hack. The insider exploited security weaknesses in both cases by using their access and knowledge of the inner systems. Even in a trusted

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

workplace, continual monitoring is necessary, as the Capital One example demonstrated, because insiders can be abused. Rather, what the Snowden case showed was that ideological beliefs may influence insider behavior in a similar way, and that businesses should consider both technological and ethical considerations when making decisions. The two incidents highlighted the need for proactive measures, such as the implementation of systems to continuously evaluate trust, the detection of anomalies, and regular audits to track any departure from the norm. To limit and lessen insider dangers, all the evidence points to the need to combine technical measures with behavioral assessment.

4.5 Cross-Model Evaluation

The researchers' proposed game-theoretic approach to detecting insider threats was tested against more traditional cybersecurity architectures in the assessment of cross-models. Because insider threats evolve over time, it became clear that traditional approaches relying on perimeter-based security and fixed trust delegations are inadequate for identifying dynamic insider threats. On the other hand, forecasting the insider's activities based on rational decision-making or, more accurately, before the dangers were known, was a significant improvement in the game-theoretic approach. The results showed that the proposed strategy was more suited for usage in contemporary decentralized work due to its increased accuracy and decreased false positive rate. This was a more proactive and proactive solution to the issue of insider threat mitigation because the game-theoretic model structure allowed for constant re-evaluation of threshold risk levels relative to the constantly updated data, giving it a significant competitive edge over conservative models.

4.6 Trust Model Outcomes

After presenting a case study on Capital One, the new game-theory based trust model obtained 92% observation accuracy and 90% accuracy in forecasting insider action. Predicting the insiders' actions, particularly in preventing questionable actions that would have led to data loss, was a breeze with the help of the model, which included simulating logical decision-making. In addition, the model significantly improved early detection, allowing cases to be identified in just 7-8 seconds. Incorporating decision-making support, the game-theoretic technique facilitated quicker responses to potential dangers, therefore reducing the exposure window. When traditional perimeter protection measures fail to meet expectations, these outcomes show that behavior-based trust models can improve cybersecurity procedures. Its results suggest that game-theoretic models might help uncover insider threats and lessen the amount of hazards more efficiently.

4.7 Observational Summary

Research also revealed a variety of unexpected trends and behavioral quirks, showing that insider threats are highly complex. Both case studies had insiders who acted in ways that would have been impossible to detect using traditional monitoring methods, such as making small but steady adjustments to data access over time. How insiders' perceptions of trust in the organization affected their actions was a major departure from theoretical assumptions. When there was a lot of trust inside a company, the insiders would take more risks since they thought no one would catch on to

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

their antics. Another trend that could be considered the most undesirable was the influence of individual beliefs; as the Snowden case demonstrates, ideological motifs had a role in determining the likelihood of classified material leaks. The information presented here suggests that businesses should handle the issue of insider behavior by considering not just technological aspects, but also psychological and ethical ones. Beyond anomalous behavior, a more thorough examination of the underlying mechanisms that lead to insider threats is necessary to determine the appropriate areas to intervene.

5. Discussion

5.1 Meaning behind the Results

The findings point to a lack of continuous dynamic trust evaluation and insufficient behavior monitoring as the primary causes of organizational problems. According to the results of the game-theoretic analysis, trustworthy insiders often misuse their access to the system without anybody noticing, particularly in situations where real-time monitoring is lacking. It is clear that companies need to replace their current, more rigid trust systems with more dynamic ones. These new systems should be able to reliably assess the risk posed by domestic actors. Strategically, game theory is useful because it can predict these dynamic relationships, which allows for better early detection and management of insider dangers. Because businesses can mimic the behaviors of their employees and the strategic decisions that lead to fixes, they may foresee potential dangers and respond accordingly before anything goes wrong.

5.2 Model Strength and Interpretation

The findings back up several key beliefs about insider threats, including those about the insider's unpredictable behavior and the long-term implications of trust erosion. Instead of looking to insiders' ill intent as the only possible explanation for their actions, game theorists have shown that they may also be accounted for by a logical assessment of the costs and benefits of the game-theoretic model. Even if insiders may act motivated by personal gain or impacted by outside forces, the model's ability to forecast their behavior at a high level demonstrates that this is still possible and will always be the case. Because of their flexibility, dynamic and behavior-based trust systems may adjust to new organizational structures and employee behaviors, lending credence to the claim that such systems are essential.

5.3 Security Applications and Policies

Incorporating the game-theoretic method with existing cybersecurity systems would be necessary to apply this concept in a real-world situation within a company. By analyzing each employee's trustworthiness in relation to their behavior and connection with sensitive systems in the firm, this model might be utilized to continuously monitor employees. When combined with other monitoring capabilities, such as user activity tracking and anomaly detection tools, it will help businesses find threats in their environments before they can damage their infrastructure. It could be helpful to integrate the model with JS regulations as well, so that dangerous workers can be recognized early on based on behavioral signs. A more proactive and comprehensive approach to

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

managing insider risks would be a part of this strategy, which would also bring HR and security strategies into harmony.

5.4 Methodological Considerations and Limits

Despite the fact that the game-theoretic approach provides valuable insights, there are certain limitations and problems associated with applying it. One of the key constraints is the data's availability or quality; dealing with insider threats before an event occurs can be difficult. Because of this, gathering comprehensive datasets for use in modeling becomes more difficult. Secondly, the complexities of human conduct, which might sometimes lunge in a different way due to distinct personalized settings or other environmental factors, may not be adequately considered by the theoretical premises of the game-theoretic approach. Scaling the approach to large firms is especially challenging because employee profiles might be diverse, making it difficult to generalize about motivations and behavior. Therefore, it is important to approach the model's predictions with care, and additional improvement is required to overcome these constraints.

5.5 Forward-Looking Insights

Improving the model's adaptability to changing organizational situations and incorporating real-time behavioral data are two areas that need further investigation for future model refinement. Human resources departments can provide more insight into employee motivations and potential triggering factors that may cause an insider threat, so it is critical that technical teams work with them to improve the accuracy of the predictions. In addition, there is room for improvement in the model by incorporating psychological and social factors that influence decision-making. This would help shed light on the motivations and behaviors of insiders. By working together, technical and HR teams can strengthen frameworks for preventing insider threats and create a safer work environment for everyone.

6. Conclusion

6.1 Recap of Major Insights

The research set out to find ways to restore faith in online security models by using game theory as a viable tool to forestall the rise of insider risks in the post-pandemic workplace. This study was quick to highlight the shortcomings of the conventional paradigm of static trust, one of which is that it fails to account for the fact that insider conduct is inherently dynamic. The study demonstrated that behavior analysis would enable better prediction of insider behaviors by combining the aspects of simulations, case studies, and expert validation. Because dynamic real-time trust models can improve the evaluation of risk levels related to the changing behaviors of users, these key findings suggest that everyone should consider dynamic real-time trust models as an important factor. By using the models, businesses may detect threats more accurately and proactively, allowing them to mitigate potential harm before it happens. The study backs up the idea that trust models need to be updated for today's decentralized workplaces, where perimeter-based protections are not as important.

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

6.2 Research Opportunities Ahead

Adding real-time data inputs to the game-theoretic technique of trust could further improve the model's accuracy and practicality in the future. Organisations may be able to better monitor and react to insider threats if this model is integrated into predictive cybersecurity systems and Security Operations Centers (SOCs). This would allow them to use real-time behavioral data to adjust security measures. To provide a more comprehensive view of insider behavior, new methods that use interdisciplinary approaches to study it from a technical, psychological, and sociological perspective are needed. In order for the model to be relevant in the evolving context of insider threat prevention, it may be necessary to investigate and improve it in the future to account for the more nuanced human motives and external influences.

References

Al-Ayed, F. (2021). "Zero-Trust Model of Cybersecurity: A Significant Challenge in the Future," 2021 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, pp. 852-854, doi: 10.1109/CSCI54926.2021.00200.

Chen, D., Chowdhury, M. M., & Latif, S. (2021). "Data Breaches in Corporate Setting," 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Mauritius, Mauritius, 2021, pp. 01-06, doi: 10.1109/ICECCME52200.2021.9590974.

Faisal, M., Ali, I., Khan, M. S., Kim, S. M., & Kim, J. (2020). "Establishment of Trust in Internet of Things by Integrating Trusted Platform Module: To Counter Cybersecurity Challenges," Complexity, 2020, 1–9, https://doi.org/10.1155/2020/6612919.

Fahim, M., & Sillitti, A. (2019). "Anomaly Detection, Analysis and Prediction Techniques in IoT Environment: A Systematic Literature Review," in IEEE Access, vol. 7, pp. 81664-81681, doi: 10.1109/ACCESS.2019.2921912.

Hanna, I. (2022). "The Snowden Files," Lau.edu.lb, http://hdl.handle.net/10725/13432.

Lang, M., & Connolly, L. (2021). "Managing the Cybersecurity Risks of Teleworking in the Post-Pandemic 'New Normal,'" SSRN Electronic Journal, https://doi.org/10.2139/ssrn.4146506.

Merrick, K., Hardhienata, M., Shafi, K., & Hu, J. (2016). "A Survey of Game Theoretic Approaches to Modelling Decision-Making in Information Warfare Scenarios," Future Internet, 8(3), 34, https://doi.org/10.3390/fi8030034.

Prabhu, S., & Thompson, N. (2020). "A Unified Classification Model of Insider Threats to Information Security," ACIS 2020 Proceedings, https://aisel.aisnet.org/acis2020/40/.

Putz, B., & Pernul, G. (2019). "Trust Factors and Insider Threats in Permissioned Distributed Ledgers," Lecture Notes in Computer Science, 25–50, https://doi.org/10.1007/978-3-662-60531-8_2.

Rass, S., König, S., & Schauer, S. (2017). "Defending Against Advanced Persistent Threats Using Game-Theory," PLOS ONE, 12(1), e0168675, https://doi.org/10.1371/journal.pone.0168675.

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

Reveraert, M., & Sauer, T. (2020). "Redefining Insider Threats: A Distinction Between Insider Hazards and Insider Threats," Security Journal, https://doi.org/10.1057/s41284-020-00259-x.

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, 9(9), 1460, https://doi.org/10.3390/electronics9091460.

Wang, Y., Wang, Y., Liu, J., Huang, Z., & Xie, P. (2016). "A Survey of Game Theoretic Methods for Cyber Security," 2016 IEEE First International Conference on Data Science in Cyberspace (DSC), Changsha, China, 2016, pp. 631-636, doi: 10.1109/DSC.2016.90.

Muniyandi, V. (2022). Harnessing Roslyn for advanced code analysis and optimization in cloud-based .NET applications on Microsoft Azure. International Journal of Communication Networks and Security, 14(4), 979-990.

Muniyandi, V. (2021). Extending Roslyn for custom code analysis and refactoring in large enterprise applications. International Journal of Science and Technology Research Archive, 3, 271-283.

Chellu, R. (2021). Secure Containerized Microservices Using PKI-Based Mutual TLS in Google Kubernetes Engine.

Chellu, R. (2022). Spectral Analysis of Cryptographic Hash Functions Using Fourier Techniques. Journal of Computational Analysis and Applications, 30(2).