A Hypergame-Theoretic Framework for Defensive Deception Against Advanced Persistent Threats

G.Swathi Reddy[1], Gowsiya Mattipati[2], Gummadi Ruthwin [3], Guruvannagari Manikanta Ashish[4], Sampangi Rajesh[5]

[1] Assistant Professor, Department of Computer Science and Engineering(AI & ML), Samskruthi College of Engineering And Technology , Kondapur(V), Ghatkesar(M), Medchal(D),Telangana

[2,3,4,5]BTech Students ,Department of Computer Science and Engineering(AI & ML), Samskruthi College of Engineering And Technology , Kondapur(V), Ghatkesar(M), Medchal(D),Telangana

***Abstract*— Defensive deception has emerged as an effective proactive strategy in cybersecurity, aiming to mislead attackers and reduce the likelihood of successful intrusions. However, many traditional game-theoretic approaches assume that both attackers and defenders share a common understanding of the system, even in uncertain conditions, which is often unrealistic. In practice, both parties operate with incomplete and asymmetric information, leading to different perceptions and decision-making processes. To address this limitation, this work presents a hypergame-based model where the attacker and defender interpret the same environment differently and select strategies based on their individual beliefs. This enables the defender to influence and manipulate the attacker's perception, which is critical in guiding their actions. The model focuses on advanced persistent threats (APTs), which involve multiple stages across the cyber kill chain, requiring adaptive and strategic responses from both sides. Simulation results demonstrate that integrating defensive deception within a hypergame framework enhances system resilience, increases the time before security failure, and improves intrusion detection accuracy with reduced false positives. Overall, the study highlights the importance of belief-driven strategies in strengthening defenses against complex, multi-stage cyber threats.**

***Keywords*— Hypergame Theory, Defensive Deception, Advanced Persistent Threats (APT), Cybersecurity, Game Theory, Intrusion Detection, Cyber Kill Chain, Threat Modeling, Proactive Defense, Network Security**

I. INTRODUCTION

In recent years, defensive deception has emerged as an effective approach in cybersecurity, aiming to mislead attackers rather than simply blocking them. By manipulating what an attacker sees or believes, defenders can increase the likelihood of incorrect decisions and failed attacks. In real-world environments, both attackers and defenders often face resource limitations, making strategic thinking essential to gain an advantage. Traditional security mechanisms, which focus only on prevention, may struggle against intelligent and adaptive threats. Deception techniques can involve hiding critical system information or deliberately presenting false data to confuse attackers [3][9]. These techniques may be passive, such as deploying hidden traps, or active, where attackers are continuously influenced during their actions. By creating uncertainty and ambiguity, defensive deception makes it significantly more difficult for attackers to achieve their goals successfully [10][13].

Game theory has been widely applied in cybersecurity to model the interactions between attackers and defenders, especially in competitive and uncertain environments. It provides a systematic way to understand how rational decision-makers select strategies to maximize their benefits [10][34]. However, traditional game-theoretic models often assume that all players have a shared and accurate understanding of the system. In practice, this assumption rarely holds true. Attackers and defenders usually operate with incomplete or uneven information, and their perceptions of the same situation may differ. These differences in understanding can strongly influence their decisions and chosen strategies. As a result, classical game theory may not fully capture the complexity and unpredictability of real-world cyber conflicts [11][32].

To overcome these limitations, hypergame theory provides a more flexible and realistic framework by considering the individual perceptions and beliefs of

different players. Unlike conventional approaches, it allows each participant to interpret the situation differently, even if those interpretations are incomplete or incorrect [5][22]. This makes hypergame theory particularly suitable for cybersecurity scenarios, where perfect information is rarely available. By taking into account uncertainty and misperceptions, it offers a deeper understanding of how attackers and defenders behave in practice. In this work, we use hypergame theory to model interactions in the presence of advanced persistent threats (APTs), which are complex, multi-stage attacks that evolve over time within the cyber kill chain [2][20].

Despite its potential, applying hypergame theory in cybersecurity is not without challenges. One key issue is the difficulty of creating realistic models that accurately represent multi-stage APT attacks beyond the initial phases. Another challenge is measuring the level of uncertainty experienced by attackers and defenders, as their perceptions directly affect their strategic decisions. Additionally, the wide range of possible strategies leads to a complex and large solution space, making analysis more demanding. Implementing deception techniques in such dynamic environments also introduces practical concerns, including cost and system complexity. Although previous studies have addressed some of these challenges, many rely on simplified models that may not scale well or fully represent real-world scenarios [12][21].

In this study, we present a hypergame-based framework to model the interaction between attackers and defenders under uncertain conditions, where each side may hold different beliefs about the same environment. The proposed model captures multiple stages of the cyber kill chain, allowing strategies to evolve dynamically over time. To manage complexity, the overall problem is divided into smaller subgames corresponding to each stage of the attack process. We also introduce a dynamic approach to estimate uncertainty based on ongoing observations and interactions, rather than relying on fixed assumptions. The effectiveness of defensive deception is evaluated using metrics such as expected utility, action cost, system lifetime, and detection accuracy. The results indicate that strategies driven by belief and perception can significantly improve system security and resilience against advanced cyber threats [4][41].

II. LITERATURE SURVEY

Aleska et al., [2016] [3] provide a detailed exploration of cybersecurity deception as a proactive defense mechanism. Their work highlights how deception techniques can be used to mislead attackers, delay intrusion attempts, and gather valuable intelligence about malicious behavior. Instead of relying solely on traditional defensive measures such as firewalls or intrusion detection systems, the authors emphasize the importance of creating uncertainty in the attacker's decision-making process. They discuss various deception strategies, including honeypots, fake data, and decoy systems, which can divert attackers away from critical assets. The study also explains how deception increases the cost and effort required for attackers to succeed, thereby discouraging persistent threats. Overall, this work demonstrates that integrating deception into cybersecurity frameworks can significantly enhance system resilience and provide defenders with a strategic advantage in dealing with sophisticated cyber-attacks.

Carroll et al., [2011] [10] examine the role of game theory in understanding and implementing deception within network security. The authors model the interaction between attackers and defenders as a strategic game, where each player aims to maximize their own benefit while anticipating the actions of the opponent. Their research shows how defenders can strategically deploy deceptive measures to influence attacker behavior, leading to suboptimal decisions by the adversary. The study introduces mathematical formulations that capture the costs and benefits associated with different strategies, providing a structured approach to analyzing security scenarios. It also demonstrates that deception can be more effective when used dynamically rather than statically. By incorporating game-theoretic principles, this work offers valuable insights into how defenders can design intelligent and adaptive security mechanisms to counter increasingly complex cyber threats.

Bennett et al., [1977] [5] introduced the concept of hypergame theory as an extension of classical game theory, focusing on situations where players may have different perceptions of the same game. Unlike traditional models that assume complete and shared information, hypergame theory accounts for misunderstandings, incomplete knowledge, and subjective beliefs. This approach is particularly useful in conflict scenarios where each participant interprets the situation differently. Bennett's work laid the foundation for analyzing strategic interactions under uncertainty, where decisions are influenced not only by actual conditions but also by perceived realities. The concept has since been widely applied in areas such as military strategy, economics, and cybersecurity. By acknowledging that players may operate under different assumptions, hypergame theory provides a more realistic framework for studying complex decision-making processes and has become an important tool

for modeling deceptive and adversarial environments.

Ferguson-Walter et al., [2019] [13] focus on the application of game theory to adaptive defensive cyber deception. Their research highlights how defenders can dynamically adjust their strategies based on the observed behavior of attackers. The authors argue that static defense mechanisms are often insufficient against advanced and persistent threats, which continuously evolve over time. By using game-theoretic models, they demonstrate how adaptive deception can mislead attackers and reduce the effectiveness of their actions. The study also explores the trade-offs between the cost of implementing deception and the security benefits gained. Through simulations and analysis, the authors show that adaptive strategies can significantly improve system security compared to traditional approaches. This work contributes to the development of intelligent defense systems that can respond in real time, making it harder for attackers to predict and exploit vulnerabilities.

Yin et al., [2013] [41] investigate optimal deceptive strategies within the framework of security games. Their work focuses on how defenders can strategically manipulate information to influence attacker decisions and improve overall system protection. The authors develop mathematical models to determine the most effective ways to allocate defensive resources while incorporating deception. They show that by carefully designing deceptive signals, defenders can mislead attackers into targeting less valuable assets, thereby minimizing potential damage. The study also considers factors such as uncertainty, resource constraints, and attacker behavior patterns. Through analytical and experimental results, the authors demonstrate that deception can significantly enhance the effectiveness of traditional security strategies. This research provides a strong foundation for designing practical cybersecurity systems that leverage deception as a key component in defending against intelligent adversaries.

III. DATASET DETAILS

The dataset used in this project is generated from a simulated Internet of Things (IoT) environment, where multiple IoT nodes continuously sense and transmit environmental data such as temperature. Each IoT device is represented as a node, and the sensed data is recorded along with attributes such as IoT ID, sensed temperature value, and timestamp. The dataset also includes user interaction details, distinguishing between legitimate users and attackers attempting unauthorized access. For genuine users, the system provides actual sensed data, whereas attackers are shown manipulated or deceptive data through honeypot mechanisms. This structure allows the system to capture both normal and malicious behaviour patterns. Additionally, all sensed data is encrypted using AES encryption to ensure security and privacy. The dataset is organized in a tabular format, making it suitable for analysis and simulation of cybersecurity scenarios, particularly for studying defensive deception techniques in IoT-based networks.

Before utilizing the dataset for analysis and system implementation, several preparation steps are performed to ensure its effectiveness. Since the data is generated dynamically from IoT simulations, it is first structured and stored in a database for easy access and management. Encryption techniques are applied to secure sensitive information, and user login data is monitored to identify potential attack patterns. The dataset is also categorized based on user behaviour, separating normal users from attackers detected by the honeypot system. Logs are maintained to record all activities, which helps in analysing attack attempts and improving defense mechanisms. Additionally, deceptive data generation is incorporated to mislead attackers, ensuring realistic simulation of cyber threats. These preprocessing and organization steps make the dataset reliable and suitable for evaluating defensive strategies, improving detection accuracy, and enhancing the overall security of the system.

IV. PROPOSED METHODOLOGY

The proposed system is designed to improve cybersecurity in an IoT environment by using defensive deception techniques. First, a simulation of IoT devices is created where multiple nodes continuously generate environmental data such as temperature. This data is securely stored after applying AES encryption to protect it from unauthorized access. A web-based interface is developed where users can register, log in, and view the IoT data. While the system is running, all user activities are carefully monitored. If a user logs in with valid credentials, they are treated as a genuine user and are allowed to access real data. However, if suspicious behavior or invalid login attempts are detected, the system identifies the user as a potential attacker. Instead of blocking them immediately, the system uses a honeypot to provide fake data, making the attacker believe they have successfully accessed the system.

After setting up the system, different types of cyber attacks such as phishing, botnet attacks, DDoS attacks, and zero-day exploits are simulated to test the system's effectiveness. For each type of attack, suitable defense mechanisms like firewalls, patch

updates, encryption key changes, and attacker removal techniques are applied. The system also maintains logs of all activities, which helps in understanding attacker behavior and improving security over time. Graphs and visual outputs are used to compare normal users and detected attackers, making it easier to evaluate performance. By combining encryption, monitoring, and deception techniques, the system provides a stronger and more intelligent defense against cyber threats while ensuring smooth access for legitimate users.

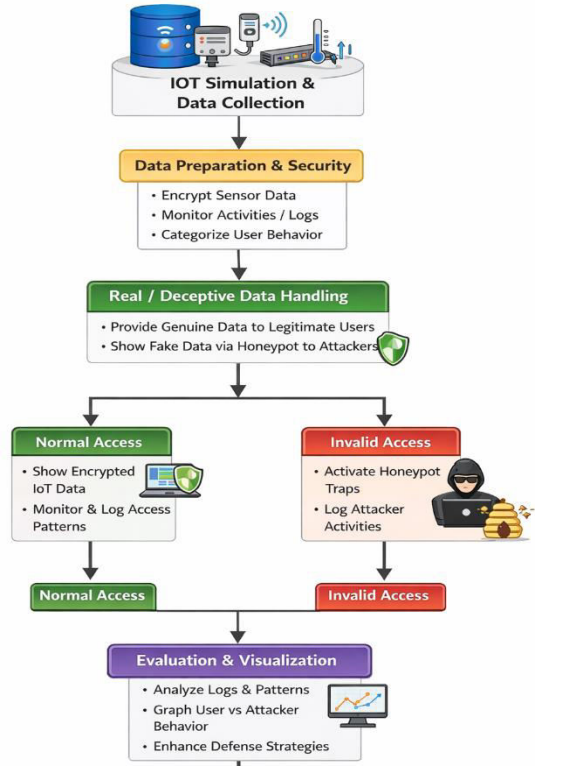

Figure [1]: Defensive Deception System in IoT Environment

Figure [1] shows the workflow of the proposed system for securing an IoT environment using defensive deception. IoT devices generate data, which is collected and secured through encryption and monitoring. The system then checks user behaviour, allowing legitimate users to access real data while redirecting attackers to a honeypot that provides fake information. Normal users can view encrypted IoT data, whereas attackers are detected and logged. Finally, the system analyses logs and visualizes results to improve security and defense strategies.

V. RESULT AND DISCUSSION

The results of the proposed system clearly show that defensive deception can effectively improve security in an IoT environment. The system is able to identify the difference between genuine users and attackers based on their login behavior. Valid users can successfully access real IoT data, while unauthorized users are not directly blocked but are redirected to a honeypot system. This honeypot provides fake but realistic data, making attackers believe they have gained access. At the same time, the system collects useful information about their activities. The use of AES encryption ensures that all IoT data remains secure during storage and transmission. Activity logs are also maintained, which helps in tracking user actions and detecting suspicious patterns. The comparison graph further shows a clear separation between normal user access and detected attacks, proving that the system can efficiently prevent unauthorized access while maintaining smooth operation for legitimate users.

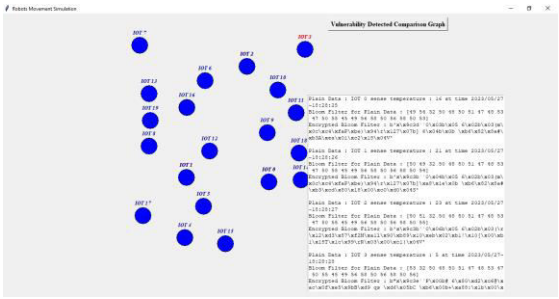

Figure [2]: IoT Simulation and Vulnerability Detection Interface

Figure [2] shows the IoT simulation where multiple devices are represented as nodes generating temperature data. The system displays both sensed data and its encrypted form. It also includes a comparison section to monitor activity and detect vulnerabilities. This helps in tracking IoT data and ensuring security within the network.

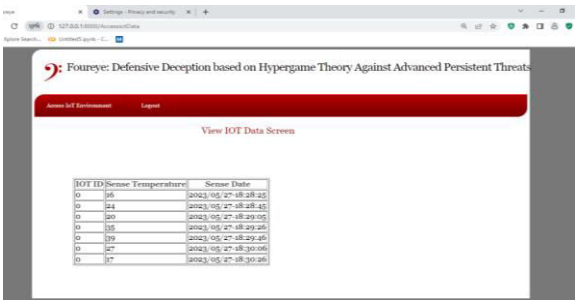

Figure [3]: IoT Data Access Interface for Legitimate User

Figure [3] shows the web application interface where a legitimate user can view IoT environment data. The data is displayed in a table format with details such as IoT ID, sensed temperature, and date-time. This screen allows users to access real-time IoT data securely after successful login.

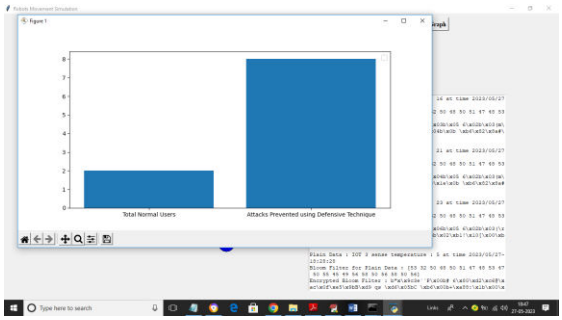

Figure [4]: Attack Detection and Prevention Comparison Graph

Figure [3] shows a graphical comparison between total normal users and the number of attacks prevented using defensive techniques. The graph clearly indicates that the system successfully detects and prevents a higher number of attacks, demonstrating its effectiveness in improving security.

DISCUSSION

The results of this project show that using deception along with traditional security methods can provide better protection in IoT systems. Instead of simply blocking attackers, the system confuses them and collects useful information about their behavior. This approach makes it harder for attackers to understand the system and carry out successful attacks. The honeypot plays an important role by diverting attackers away from real data. At the same time, encryption ensures that sensitive information remains safe. The logging system helps in analyzing attack patterns and improving future security measures. Compared to basic security techniques, this method adds an extra layer of intelligence by influencing attacker decisions. Overall, the project proves that combining monitoring, encryption, and deception can significantly strengthen the security of IoT networks.

VI. CONCLUSION

This project successfully demonstrates the use of defensive deception techniques to enhance security in an IoT environment against advanced persistent threats. By implementing mechanisms such as AES encryption, user monitoring, and honeypot systems, the network is protected from unauthorized access. The system effectively distinguishes between legitimate users and attackers based on their behavior. Genuine users are allowed to access real IoT data, while attackers are redirected to a deceptive environment where fake data is provided. This approach not only prevents attacks but also helps in collecting valuable information about attacker activities. Visualization tools such as graphs further help in analysing system performance and attack detection. The results show that the proposed system can efficiently detect, mislead, and control malicious users. Overall, this project highlights the importance of combining security techniques like encryption, monitoring, and deception to build a strong and reliable IoT security framework, and it provides a solid foundation for future enhancements and real-world implementation.

REFERENCES

[1] “Common vulnerability scoring system (CVSS).” [Online]. Available: https://www.first.org/cvss/

[2] Y. M. Allegri, M. A. Bashar, L. Fang, and k. W. Happel, “First-level hyper game for investigating misperception in conflicts,” IEEE Trans. Systems, Man, and Cybernetics: Systems, vol. 48, no. 12, pp. 2158–2175, 2017.

[3] H. Aleska and H. Spafford, “Cyber security deception,” in Cyber Deception. Springer, 2016, pp. 25–52.

[4] C. Bakker, A. Bhattacharya, S. Chatterjee, and D. L. Vrabie, “Learning and information manipulation: Repeated hypergamic for cyber-physical security,” IEEE Control Systems Letters, vol. 4, no. 2, pp. 295–300, 2019.

[5] P. G. Bennett, “Toward a theory of hyper games,” Omega, vol. 5, no. 6, pp. 749–751, 1977.

[6] E. Bertino and N. Islam, “Botnets and Internet of Things security,” Computer, vol. 50, no. 2, pp. 76–79, Feb. 2017.

[7] M. Brossard, D. T. Bui, L. Ciavaglia, R. Douville, M. L. Palac, N. L. Suze, L. Nouria, S. Papillon, P. Peloso, and F. Santoro, “Software-defined LANs for interconnected smart environment,” in 2015 27th Int’l Tele traffic Congress, Sep. 2015, pp. 219–227.

[8] U. Brandes, “A faster algorithm for betweenness centrality,” Jour. mathematical sociology, vol. 25, no. 2, pp. 163–177, 2001.

[9] J. W. Caddell, “Deception 101-primer on deception,” DTIC Document, Tech. Rep., 2004.

[10] T. E. Carroll and D. Grosu, “A game theoretic investigation of deception in network security,” Security and Communication Networks, vol. 4, no. 10, pp. 1162–1172, 2011.

[11] W. Casey, A. Kellner, P. Mimar mosher, J. A. Morales, and B. Mishra, “Deception, identity, and

security: The game theory of Sybil attacks," Comms. of the ACM, vol. 62, no. 1, pp. 85–93, 2018.

[12] J.-H. Cho, M. Zhu, and M. P. Singh, Modeling and Analysis of Deception Games based on hypergamic Theory. Cham, Switzerland: Springer Nature, 2019, Ch. 4, pp. 49–74.

[13] K. Ferguson-Walter, S. Fugate, J. Mauger, and M. Major, "Game theory for adaptive defensive cyber deception," in Proc. 6th Annual Symp. on Hot Topics in the Science of Security. ACM, 2019, p. 4.

[14] N. M. Fraser and K. W. Happel, Conflict Analysis: Models and Resolutions. North-Holland, 1984.

[15] N. Garg and D. Grosu, "Deception in honeynets: A game-theoretic analysis," in Proc. IEEE Information Assurance and Security Workshop (IAW). IEEE, 2007, pp. 107–113.

[16] B. Harsimar and J. Cortes, "Evolution of the percept- ´ Tion about the opponent in hyper games," in Proc. 49th IEEE Conf. Decision and Control (CDC), Dec. 2010, pp. 1076–1081.

[17] ——, "Evolution of players' misperceptions in hyper games under perfect observations," IEEE Trans. Automatic Control, vol. 57, no. 7, pp. 1627–1640, Jul. 2012.

[18] I. GmbH. Mind Node. [Online]. Available: https: //mindnode.com/

[19] J. Han, J. Pei, and M. Kamber, Data Mining: Concepts and Techniques. Elsevier, 2011.

[20] J. T. House and G. Benko, "hypergamic theory applied to cyber-attack and defense," in Proc. SPIE Conf. Sensors, and Command, Control, Comms., and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense IX, vol. 766604, May. 2010.

[21] T. Kanazawa, T. Ushio, and T. Yamasaki, "Replicator dynamics of evolutionary hyper games," IEEE Trans. Systems, Man, and Cybernetics - Part A: Systems and Humans, vol. 37, no. 1, pp. 132–138, Jan. 2007.