



A Blockchain-Based Decentralized Social Networking Platform

Syed Althaf¹, Syed Liyaqath Ullah², Mohd Riyan³, Shaik Saifuddin⁴, Sheikh Hamdan Al Amoudi⁵

¹Assistant Professor, Department of CSE (Data Science), Lords Institute of Engineering and Technology, Hyderabad, Telangana, India.

^{2,3,4,5}UG Students, Department of CSE (Data Science), Lords Institute of Engineering and Technology, Hyderabad, Telangana, India.

Abstract— Cybersecurity systems today largely depend on reactive mechanisms that identify known threats but often fail against sophisticated attacks like Advanced Persistent Threats (APTs). These attackers operate stealthily and adapt over time, making traditional defenses insufficient. This work proposes a novel Hypergame Theory-Based Defensive Deception Model, called “Four Eyes,” designed to proactively counter such threats. The system models cyber conflict by considering differences in perception between attackers and defenders, enabling the creation of intelligent deception strategies. By introducing misleading information and dynamically adapting based on attacker behavior, the system disrupts malicious activities and reduces the risk of long-term breaches. Additionally, integration with blockchain ensures secure storage and transparency of critical documents, preventing tampering and unauthorized access. The proposed approach enhances system resilience, improves decision-making capabilities, and provides a robust defense framework against evolving cyber threats in modern digital environments.

Keywords— Cybersecurity, Advanced Persistent Threats (APTs), defensive deception, hypergame theory, blockchain technology, proactive defense, intrusion detection systems, data integrity, secure document management, game theory.

I. INTRODUCTION

With the rapid growth of digital technologies, cybersecurity has become a critical concern for both organizations and individuals. Traditional security mechanisms such as firewalls, intrusion detection systems (IDS), and signature-based

detection techniques—have been widely used to protect systems from malicious attacks.

However, these approaches are largely reactive, meaning they respond only after a threat has been identified [1], [7]. This limitation becomes particularly problematic when dealing with Advanced Persistent Threats (APTs), which are highly sophisticated and capable of remaining undetected within systems for extended periods [3].

APTs are designed to continuously evolve, adapt, and exploit system vulnerabilities, making them difficult to detect using conventional methods. Attackers often analyze system behavior and dynamically modify their strategies, posing a significant challenge for defenders [10]. While several studies have explored the use of game theory to model interactions between attackers and defenders, these models often assume perfect information and fully rational decision-making [5], [6]. In real-world scenarios, however, both attackers and defenders operate under uncertainty, incomplete knowledge, and subjective perceptions, which limits the effectiveness of classical game-theoretic approaches [8], [9].

To address these challenges, modern cybersecurity research is shifting toward proactive defense strategies. One promising approach is defensive deception, where systems intentionally mislead attackers by presenting false information or creating decoy environments. This technique not only delays attackers but also provides valuable insights into their behavior and strategies [1], [2], [19].

In addition to security challenges, ensuring data integrity and secure storage has become increasingly important, particularly for sensitive digital assets such as legal documents and social media data.



Blockchain technology offers a decentralized and tamper-resistant solution for secure data management. By recording document transactions in an immutable ledger, blockchain ensures transparency, traceability, and integrity of stored information.

This project integrates hypergame theory-based deception with blockchain technology to develop a robust and intelligent cybersecurity framework. The proposed system enhances defense against advanced threats while ensuring secure and trustworthy document management, making it highly suitable for modern digital applications [3], [13].

The system models cyber conflict by considering differences in perception between attackers and defenders, enabling the creation of intelligent deception strategies. By introducing misleading information and dynamically adapting based on attacker behavior, the system disrupts malicious activities and reduces the risk of long-term breaches.

Additionally, integration with blockchain ensures secure storage and transparency of critical documents, preventing tampering and unauthorized access. The proposed approach enhances system resilience, improves decision-making capabilities, and provides a robust defense framework against evolving cyber threats in modern digital environments.

II. RELATED WORK

Al-Shaer, E. (2016). Deception in Cybersecurity: Techniques and Applications. Al-Shaer's book provides a comprehensive exploration of deception techniques in cybersecurity, emphasizing their role in proactive defense strategies. The work discusses various deception mechanisms such as honeypots, honeytokens, and moving target defenses, which are designed to mislead attackers and delay their progress. It highlights how traditional reactive security systems fail to handle sophisticated threats effectively and proposes deception as a means to enhance situational awareness. The book also explains how deceptive environments can be strategically designed to gather intelligence about attacker behavior, thereby improving defense planning. It

presents practical implementation techniques and real-world case studies, demonstrating the effectiveness of deception in modern cyber defense. [1]

Pawlick, J., Colbert, E., & Zhu, Q. (2019). A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy. This paper presents a detailed survey and taxonomy of defensive deception techniques in cybersecurity using a game-theoretic perspective. The authors categorize various deception strategies based on their objectives, such as perturbation, obfuscation, and misdirection. It emphasizes the importance of modeling attacker-defender interactions as strategic games, where both parties continuously adapt their strategies. The paper also identifies gaps in existing research, particularly the limitations of assuming perfect rationality and complete information in traditional game models. This survey is valuable for understanding the theoretical foundations of cyber deception and supports the development of more realistic and adaptive defense mechanisms in cybersecurity systems.[2]

Shen, C., Wei, J., & Liu, Y. (2021). Hypergame theory-based proactive defense for APTs in cyber systems. Unlike classical game theory, hypergame theory accounts for differences in perception between attackers and defenders, making it more suitable for real-world cybersecurity scenarios. The authors propose a multi-stage defense model where defenders strategically deploy deception techniques to mislead attackers and influence their decision-making processes. The study demonstrates how hypergame models can effectively capture uncertainty, incomplete information, and cognitive biases in cyber conflicts. This work is highly relevant as it bridges the gap between theoretical modelling practical cybersecurity challenges, providing a strong foundation

for developing intelligent and adaptive defense systems based on perception-aware strategies.[3]

Huang, L., Wang, J., Li, X., & Zhang, T. (2020). Modeling multi-stage APTs using dynamic Bayesian networks and game theory. This paper focuses on modeling multi-stage Advanced Persistent Threats (APTs) using dynamic Bayesian networks combined with game theory. The authors present a framework that captures the sequential and probabilistic nature of APT attacks, where attackers move through different stages such as reconnaissance, intrusion, and data exfiltration. By integrating game theory, the model enables defenders to anticipate attacker strategies and make optimal defense decisions. The study highlights the importance of understanding dependencies between different attack stages and how uncertainty affects decision-making. It also provides quantitative methods for risk assessment and defense planning. Experimental results demonstrate that the proposed approach improves the accuracy of attack prediction and enhances system resilience. [4]

IV. PROPOSED METHODOLOGY

The proposed method introduces an intelligent cybersecurity framework that integrates hypergame theory-based defensive deception with blockchain technology to effectively counter Advanced Persistent Threats (APTs). The system is designed to operate proactively by predicting attacker behavior and dynamically adapting defense strategies based on perceived threats and uncertainties.

Initially, the framework models the interaction between attackers and defenders using hypergame theory, which considers incomplete information and differing perceptions of both parties. Unlike traditional game-theoretic models, this approach captures real-world scenarios where attackers may have limited knowledge about the system, and defenders may misinterpret attacker intentions. Based on this model, multiple defense strategies are generated and evaluated to determine optimal responses under varying conditions.

To enhance system security, defensive deception techniques are incorporated, including the deployment of honeypots, decoy networks, and misleading information. These mechanisms are designed to confuse attackers, delay intrusion attempts, and collect behavioral data for further analysis. The insights gained are continuously fed back into the system to refine defense strategies, creating an adaptive learning loop. In parallel, blockchain technology is utilized to ensure secure and tamper-proof storage of sensitive documents and system logs. Each transaction or document record is stored as an immutable block, providing transparency, traceability, and data integrity.

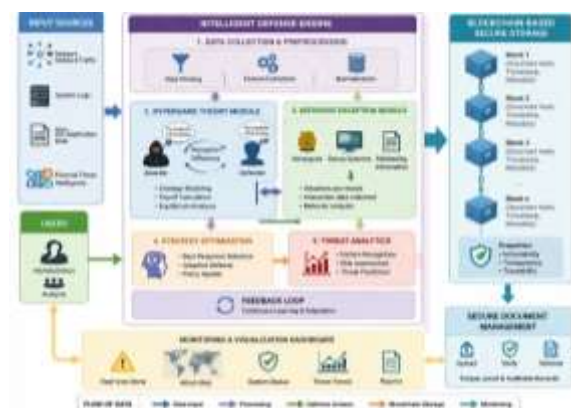


Figure [1] : System Architecture

The system architecture diagram illustrates a comprehensive cybersecurity framework that integrates hypergame theory, defensive deception, and blockchain technology to provide proactive and secure protection against advanced threats. It begins with multiple input sources, including network traffic, system logs, user data, and external threat intelligence. These inputs are processed within the Intelligent Defense Engine, where data undergoes filtering, feature extraction, and normalization. The architecture then applies a hypergame theory module, which models attacker-defender interactions under incomplete information, capturing perception differences and enabling strategic decision-making. Alongside this, the defensive deception module deploys mechanisms such as honeypots, decoy systems, and misleading information to confuse attackers and gather behavioral insights. The system then performs strategy optimization to select the best defensive actions, followed by threat analytics for pattern recognition, risk assessment, and prediction. A continuous feedback loop ensures adaptive learning and system improvement over time. The framework also integrates blockchain-based secure storage, where document data and logs are stored

as immutable blocks, ensuring transparency, traceability, and data integrity. Finally, the architecture includes a monitoring and visualization dashboard, allowing administrators and analysts to track system status, receive real-time alerts, and analyze threat trends effectively.

V.RESULT AND DISCUSSION

The implementation of the QR-based food ordering system demonstrates significant improvements in restaurant operations and customer experience. The system successfully reduces order processing time by allowing customers to directly place orders through their smartphones without waiting for staff assistance. This leads to faster service, especially during peak hours. Additionally, the accuracy of orders is greatly improved, as customers select items themselves, minimizing miscommunication and human errors. The digital menu feature enables easy updates and better presentation of food items, enhancing customer interaction. The integration of online payment methods ensures secure and convenient transactions, reducing the need for cash handling. Restaurant owners can monitor orders in real time, track sales, and manage menu updates efficiently. The system also provides better organization in the kitchen by sending orders directly to the kitchen display. Overall, the results indicate that the system improves operational efficiency, enhances customer satisfaction, and reduces workload on staff. It proves to be a reliable and scalable solution for modern restaurants seeking to adopt digital transformation contactless services.

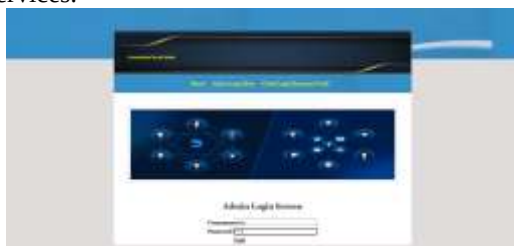


Figure [2] : Admin Login

Figure [2] admin can login to system using username and password as 'admin'.



Figure [3] : Upload Document

Figure [3] Entering some type of Political News document details and then upload related document data.



Figure [4] : Downloading Data

Figure [4] illustrates right side panel can see downloading of associated data. Now logout and then normal users can view all available documents but we are granting to them to document details but cannot download associated data.

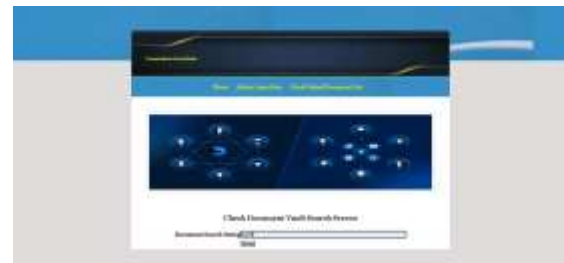


Figure [5] : Check Document

Figure [5] illustrates user can enter any string like person name about to search, document UID number or any other text. Entered input will be matched with available documents in Blockchain and get below result.

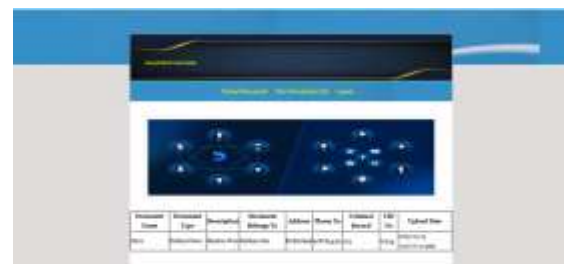




Figure [6] : Query user

Figure [6] illustrates query user can see one search found and users are granting to view above details and cannot download associated document file.

DISCUSSION

The proposed cybersecurity framework highlights the importance of shifting from reactive to proactive defense mechanisms in addressing modern cyber threats, particularly Advanced Persistent Threats (APTs). Traditional security approaches, while effective against known threats, lack the adaptability required to counter evolving and stealthy attacks. By incorporating hypergame theory, the system accounts for incomplete information and varying perceptions between attackers and defenders, offering a more realistic representation of cyber conflicts. This enables defenders to anticipate adversarial behavior and strategically deploy countermeasures. The integration of defensive deception further strengthens the framework by misleading attackers through decoy systems and false information. This not only delays potential breaches but also allows the collection of valuable intelligence on attacker strategies. Additionally, the use of blockchain technology enhances data integrity and secure document management by ensuring immutability and transparency. However, implementing such a system introduces challenges, including increased computational complexity, resource requirements, and the need for careful design of deception strategies to avoid detection. Despite these limitations, the combined approach provides a scalable and intelligent solution for modern cybersecurity challenges, offering improved resilience against sophisticated and persistent threats.

VI. CONCLUSION

In conclusion, this project presents a comprehensive cybersecurity framework that combines hypergame theory-based deception with blockchain technology to address the limitations of traditional security systems. The study demonstrates that reactive defense mechanisms are insufficient for handling sophisticated threats such as Advanced Persistent Threats (APTs), which require adaptive and intelligent solutions. By leveraging hypergame theory, the proposed system effectively models real-world attacker-defender

interactions under uncertainty and incomplete information, enabling more informed and strategic defense decisions. The incorporation of defensive deception techniques enhances the system's ability to mislead attackers, delay intrusions, and gather critical insights into adversarial behavior. Furthermore, blockchain technology ensures secure and tamper-proof storage of sensitive data, addressing concerns related to data integrity and trust. Overall, the integration of these technologies results in a robust, proactive, and resilient cybersecurity framework. Future work can focus on optimizing system performance, reducing implementation complexity, and exploring real-world deployment scenarios. This approach has significant potential for securing modern digital infrastructures and protecting critical information systems against increasingly cyber threats.

REFERENCES

1. Al-Shaer, E. (2016). *Deception in Cybersecurity: Techniques and Applications*. Springer.
2. Pawlick, J., Colbert, E., & Zhu, Q. (2019). A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy. *ACM Computing Surveys (CSUR)*, 52(4).
3. Shen, C., Wei, J., & Liu, Y. (2021). Hypergame theory-based proactive defense for APTs in cyber systems. *IEEE Access*, 9, 11534–11547.
4. Huang, L., Wang, J., Li, X., & Zhang, T. (2020). Modeling multi-stage APTs using dynamic Bayesian networks and game theory. *Future Generation Computer Systems*, 107, 544–555.
5. Durkota, K., Lisy, V., Bošanský, B., & Kiekintveld, C. (2017). Game-theoretic models for security analysis of networked systems. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 8(4), 1–29.
6. Zhu, Q., & Başar, T. (2013). Game-theoretic methods for robustness,



- security, and resilience of cyberphysical control systems: Games-in-games principle for optimal cross-layer resilient control systems. *IEEE Control Systems Magazine*, **35**(1), 46–65.
7. Roy, A., Ellis, C., Shiva, S., Dasgupta, D., & Shandilya, V. (2010). A survey of game theory as applied to network security. In *Proceedings of the 43rd Hawaii International Conference on System Sciences*, 1–10.
8. Carroll, T. E., & Grosu, D. (2011). A game theoretic investigation of deception in network security. *Security and Communication Networks*, **4**(10), 1162–1172.
9. Alpcan, T., & Başar, T. (2010). *Network security: A decision and game-theoretic approach*. Cambridge University Press.
10. Wang, W., Lu, Z., Lu, X., & Liu, J. (2020). From attack graph to defense graph: Security assessment and defense planning for industrial control systems. *IEEE Transactions on Industrial Informatics*, **16**(2), 1021–1030.
11. Amin, S., Schwartz, G. A., & Sastry, S. (2013). Security of interdependent and identical networked control systems. *Automatica*, **49**(1), 186–192.
12. Sengupta, S., Chowdhary, A., Sabur, A., & Zhan, J. (2018). A survey of moving target defenses for network security. *IEEE Communications Surveys & Tutorials*, **22**(3), 1989–2016.
13. Han, Y., Zhao, X., & Liu, Y. (2020). A dynamic game approach to deception-based cyber defense strategy optimization. *IEEE Access*, **8**, 65959–65969.
14. Kott, A., & Arnold, C. (2013). *Cyber defense and situational awareness*. Springer.
15. Liu, P., Singhal, A., & Wijesekera, D. (2015). Game theory for cyber deception: Framework and case study. In *Cyber Deception* (pp. 93–118). Springer.
16. Cardenas, A. A., Amin, S., & Sastry, S. (2008). Research challenges for the security of control systems. In *HotSec*.
17. Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, **86**, 13–23.
18. Liu, Y., Xiao, Y., & Li, S. (2012). Cyber security and privacy issues in smart grids. *IEEE Communications Surveys & Tutorials*, **14**(4), 981–997.



19. Heckman, C., Walsh, R., Stech, F., Thomas, R., & Heckman, K. (2015). Active cyber defense with denial and deception: A cyber-wargame experiment. *Computers & Security*, **37**, 72–77.
20. Grossklags, J., Christin, N., & Chuang, J. (2008). Secure or insure? A game-theoretic analysis of information security games. In *Proceedings of the 17th international conference on World Wide Web* (pp. 209–218).
21. Babburi, S. Privacy-Preserving Collaborative Framework with Auditable Federated Learning.
22. Gaddam, S. Integrating Analytics into the Development Process: Bridging the Gap between Data Insights and Design Execution.
23. Immadi, S. K. (2025). Optimizing ERP for Human Capital Management. *Applied Research for Growth, Innovation and Sustainable Impact*, 377–384.
<https://doi.org/10.1201/9781003684657-63>
24. Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
25. Poojari, R. INTELLIGENT SYSTEMS+B108 AND APPLICATIONS IN ENGINEERING.
26. Mahimalur, R. K., Vasgam, M., & Manoharan, D. Devops Lifecycle Management And Cloud Migration Assessments: A Security-Driven CICD Perspective.
27. Viswanathan, V. (2023). AI-Augmented Decision Intelligence for Enterprise Systems: Integrating Cognitive Analytics for Resource and Talent Optimization.
28. Agrawal, A. M., Gajula, S., Shinde, R. P., Shah, H., & Ghosh, H. (2025, July). Machine Translation for Long Sequences with Enhanced Attention Mechanisms. In *2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET)* (pp. 1-6). IEEE.
29. Maturi, S. Y. (2021). Blockbond hardening: Securing pooled-hash protocols against traffic tampering, MITM hash-rate hijacking, and template coercion. *International Journal of Communication Networks and Information Security*, **13**(3), 718–728.
30. Adabala, P. K. (2024). Utilizing predictive analytics to improve efficiency and decision-making in ERP-connected supply chains. *International Journal of Intelligent Systems and Applications in Engineering*, **12**(22s), 2465
31. Kavuri, S. (2026). An Explainable Machine Learning Framework for Predicting Software Defects in Large-Scale Software Systems. *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*, 1–6.
<https://doi.org/10.1109/icaic67076.2026.11395777>
32. Venkata Pavan Kumar Gummadi. (2023). MuleSoft Batch Processing: High-Volume Streaming Architecture. *Computer Fraud and Security*, 50–57.
<https://doi.org/10.52710/cfs.886>
33. Shashank, A. (2025). Self-Healing Data Pipelines for Enhanced Reliability: A Paradigm Shift in Enterprise Data Management. *Journal of Computer Science and Technology Studies*, **7**(8), 1097-1104.
34. Susarla, R. S., Boyapati, P. K., & Kandula, S. T. R. (2025, July). Cloud-Based Secure Data Storage in Smart Cities Using Central-Smoothing Hypergraph Neural Networks. In *2025 IEEE 4th World Conference on Applied Intelligence and Computing (AIC)* (pp. 279-284). IEEE.
35. Boyapati, P. K. Building a centralized data operations hub for healthcare enterprise integration. *IJSAT-Int. J. Sci. Technol.* **16** (2).

