Review Paper on "Big Holy Framework - A Game Changer for Cybersecurity?"

Kishor SB[1] and Sunil Kashibarao Nayak[2]

Head, Dept. of Computer Science, SP College, Chandrapur, Maharashtra, India
Head, Department of Computer Science, Bahirji Smarak Mahavidyalaya, Basmathnagar Dist-Hingoli MS, India.
Email: [1]sbk.social30@gmail.com | [2]sunilnayak1234@yahoo.com

Manuscript Details

Available online on https://www.irjse.in
ISSN: 2322-0015

Editor: Dr. Arvind Chavhan

Cite this article as:
Kishor SB and Sunil Kashibarao Nayak. Review Paper on "Big Holy Framework - A Game Changer for Cybersecurity?, *Int. Res. Journal of Science & Engineering,* 2024, Special Issue A14: 19-21. https://doi.org/10.5281/zenodo.12699231

Article published in Special issue of National Conference on Machine Learning and Data Science (NCMLDS-2024)" organized by College of Computer Science and Information Technology (COCSIT) Ambajogai Road, Latur, Maharashtra, India on date April 16th to 17th 2024

Abstract

This study delves into the potential of a novel framework called the "Big Holy" game for cybersecurity and threat detection. This framework leverages the combined strengths of four key intelligence sources: Artificial Intelligence (AI), Human Intelligence (HI), hidden intelligence (encompassing human unconscious cognition and intuition), and Data Intelligence.

Keywords: Artificial Intelligence (AI), Human Intelligence (HI), hidden intelligence, Cycber security.

Introduction

Imagine a powerful new way to fight cyber threats! This approach is called the "Big Holy" game, and it's all about working together. Here's the team:

- **Super Smart Machines** (AI): These whizzes can crunch data like nobody's business, spotting patterns humans might miss.
- **Clever People** (Human Intelligence): We bring the experience and know-how to understand what those patterns mean and make tough calls.
- **Gut Feelings** (Hidden Intelligence): Sometimes our hunches can be right on the money. This game taps into that intuition.
- **Data Detectives** (Data Intelligence): All the info we collect is a goldmine for spotting threats.

Cybersecurity threats are like sneaky ninjas, always changing tactics [1] . By working together, this all-star team (AI, Human Intelligence, Hidden Intelligence, and Data Intelligence) can be much stronger than any one of them alone. We believe this "Big Holy" game can dramatically improve how we detect and fight cyber threats.

This paper explores a novel concept, the "Big Holy" framework, to revolutionize cybersecurity threat detection. The framework advocates for a collaborative approach, integrating four key ethical intelligence sources.

- **Artificial Intelligence (AI):** The power of machines for data analysis and pattern recognition.
- **Human Intelligence (HI):** Our experience and knowledge for contextual understanding and decision-making.
- **Hidden Intelligence (HI):** The role of human intuition and unconscious cognition in threat detection (Author Name(s), Year).

Data Intelligence (DI): The insights gleaned from the vast amount of data collected in cybersecurity. The core idea behind the Big Holy game is to leverage the strengths of each intelligence type to create a more robust and adaptable cybersecurity posture, a critical factor in today's ever-evolving threat landscape where traditional methods relying on individual intelligence sources may prove insufficient. [2]

Strengths of the Big Holy Framework

- **Comprehensiveness:** The framework encompasses a wider range of intelligence sources than traditional approaches, potentially leading to a more holistic understanding of threats
- **Synergy:** Collaboration between AI, HI, hidden intelligence, and DI can foster better decision-making by combining analytical power with human expertise and intuition
- **Adaptability:** The framework's flexibility allows for continuous learning and improvement as new threats emerge and technologies evolve

Research Considerations

- The paper proposes a mixed-methods approach to evaluate the Big Holy framework. This is commendable, as a case study combined with interviews with cybersecurity professionals can provide valuable insights into the framework's feasibility and potential impact. [3]
- However, further research is necessary to address some key areas:
- **Integration Techniques:** The paper acknowledges the need for specific techniques to integrate these diverse intelligence sources. Research into effective methods for achieving this seamless collaboration is crucial.
- **Ethical Considerations:** The use of AI and hidden intelligence in cybersecurity raises ethical concerns. Research should explore ways to mitigate potential biases and ensure responsible implementation.
- **Metrics for Success:** Developing clear metrics to measure the effectiveness of the Big Holy framework in threat detection and response is essential.

Conclusion

The Big Holy framework presents a promising approach to cybersecurity by harnessing the collective power of AI, HI, hidden intelligence, and DI. We still need to do more research to understand how to mix different techniques, ensure everything is done ethically, and measure how successful it is. However, if we can figure these things out, working together in this way could have a huge impact on our ability to combat cyber threats effectively.

This collaborative approach brings together different ideas, expertise, and resources from various fields and organizations. By integrating these diverse perspectives and strategies, we can develop more comprehensive and robust solutions to cybersecurity challenges. Moreover, this framework emphasizes ethical considerations, ensuring that our actions are morally sound and respect privacy rights and human values.

Furthermore, establishing clear metrics for success allows us to evaluate the effectiveness of our efforts and make necessary adjustments. By quantifying outcomes and progress, we can identify areas for improvement and refine our strategies over time. Ultimately, the potential benefits of this collaborative approach are significant, as it holds the promise of enhancing our collective cybersecurity posture and safeguarding critical systems and data from malicious actors.

References

1. S. K. Hassan and A. Ibrahim, “The role of Artificial Intelligence in Cyber Security and Incident Response:,” International Journal for Electronic Crime Investigation, vol. 7, no. 2, Art. no. 2, Jul. 2023, doi: 10.54692/ijeci.2023.0702154.
2. S. S. Rajest, B. Singh, A. J. Obaid, R. Regin, and K. Chinnusamy, Advances in Artificial and Human Intelligence in the Modern Era. IGI Global, 1AD. Accessed: Mar. 17, 2024. [Online]. Available: https://www.igi-global.com/book/advances-artificial-human-intelligence-modern/www.igi-global.com/book/advances-artificial-human-intelligence-modern/327347
3. L. Floridi, The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities. Oxford University Press, 2023.

Conflicts of interest: The authors stated that no conflicts of interest.

Publisher’s Note
IJLSCI remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Correspondence and requests for materials should be addressed to Sonali Gaikwad.

Peer review information
IRJSE thanks the anonymous reviewers for their contribution to the peer review of this work. A peer review file is available.

Reprints and permissions information is available at https://www.irjse.in/reprints