IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Designing And Evaluation User Experience Of An AI-Based Defense System

Faiz Khan, Himanshu Dhurve, Nikhil Kakar, Prof. Anuradha Kale
Leader, Member 1, Member 2 Guide
Department Of Computer Science And Engineering
Prof. Ram Meghe College Of Engineering And Management, Badnera, Maharashtra

Abstract

— The rapid integration of artificial intelligence into modern defense systems has significantly enhanced threat detection, decision making, and operational efficiency. However, the effectiveness of such systems is determined not merely by algorithmic performance but also by the quality of user experience provided to human operators. Poor usability, lack of transparency, and explainability may reduce trust and hinder effective human-AI collaboration in high-risk defense environments. This research focuses on the design and evaluation of user experience in an AI-based defense system from a human-centered approach.The proposed system incorporates AI driven threat analysis with a priority on usability, interpretability, and operator trust. A structured UX framework is developed by integrating principles of human-computer interaction, explainable AI, and usability engineering. The evaluation is quantitative usability performed through both and qualitative approaches: testing, task-based performance analysis, and user satisfaction surveys. Key UX parameters are investigated, including ease of use, system transparency, response time, and decision confidence.Experimental results reflect that the optimized UX design significantly improves operator efficiency, situational awareness, and trust in AI-assisted decision making. The findings demonstrate that incorporating UX-oriented design principles into AI-based defense systems enhances both system effectiveness and human performance. This study underlines the importance of human-centric design in defense technologies and provides valuable insights for the development of reliable, usable, and trustworthy AI-driven defense systems.

I. INTRODUCTION

The pace of development of AI has changed the face of modern defense with its intelligent detection of threats, automated decision support, and real-time situational awareness. Applications of AI in defense are expanding into vital areas like cybersecurity, surveillance, autonomous monitoring, and strategic decision making. Such systems process volumes of data at high speeds with accuracy and thereby provide immense advantages compared to traditional rule-based defense mechanisms. Nevertheless, their technical sophistication notwithstanding, the successful implementation of AI-driven defense systems depends heavily on effective interaction between human operators and intelligent systems. In high-risk defense, human operators retain responsibility for supervision, validation, and making decisions. Poor usability, lack of transparency, and complex interfaces have adverse impacts on operator performance, situational awareness, and trust in AI-assisted outputs. Many current AI-driven defense systems emphasize algorithmic accuracy and automation at the expense of UX factors like usability, interpretability, and cognitive workload. This gap frequently results in degraded operational reactions, and efficiency, slower possible decision errors, especially under time-critical conditions in defense.

User experience is critical to effective human AI collaboration. Well-designed UX allows operators to understand system behavior, interpret AI-generated insights, and confidently act upon recommendations. Key UX factors such as ease of use, system responsiveness, explainability, and trust are essential for ensuring AI-based defense systems support, rather than hinder, human decision-making. Thus, incorporating human-centered design principles into defense technologies is paramount to ensuring that AI systems can be reliable, transparent, and user-friendly.

This research approaches the design and evaluation of an AI-based defense system using a structured, human-centered approach to user experience. A UX-oriented framework is proposed where integration between principles of human-computer interaction, explainable AI, and usability engineering has been ensured. The system is evaluated through both qualitative and quantitative means: usability testing, task performance analysis, and user satisfaction assessment. This study will seek to find design strategies that improve operators' trust, usability, and efficiency in decision-making by exploring key UX parameters.

The paper has three important contributions: It revisits the importance of UX as a crucial factor affecting the effectiveness in AI-based defense systems; it proposes a structured approach for the design of user-oriented AI defense interfaces. Third, it provides empirical results of an evaluation that shows how improved UX design positively influences human performance and system reliability. As a result, this study offers important insights to researchers, system designers, and defense practitioners who are interested in developing robust, trustworthy, and human-centered AI based defense solutions.

II. LITREATURE REVIEW

The increasing adoption of artificial intelligence (AI) in defense systems has attracted significant research attention over the past decade. AI-driven defense technologies are widely applied in areas such as cybersecurity, surveillance, autonomous systems, and decision support, where rapid data processing and accurate threat identification are critical. While substantial progress has been made in improving algorithmic accuracy and system automation, recent studies highlight that the effectiveness of AI-based defense systems also depends heavily on user experience (UX) and human–AI interaction.Several researchers have explored the role of AI in enhancing defense capabilities. Studies on AI-based threat detection systems demonstrate that machine learning and deep learning models outperform traditional rule-based methods in identifying complex and evolving threats. These systems are capable of analyzing large-scale data streams in real time, enabling proactive defense mechanisms.

However, despite their technical advantages, researchers report challenges related to system transparency, explainability, and operator trust, particularly in high-stakes defense environments where incorrect decisions can have severe consequences.User experience and usability have been widely studied in the broader context of human computer interaction (HCI). Prior research emphasizes that well-designed interfaces improve task efficiency, reduce cognitive load, and enhance user satisfaction. In AI driven systems, the lack of explainability and opaque decision-making processes— often referred to as the “black-box” problem—have been identified as major barriers to user trust. Studies on explainable AI (XAI) suggest that providing clear explanations of AI outputs significantly improves user understanding and confidence, especially in safety-critical domains such as defense and cybersecurity.In the context of defense systems, human–AI collaboration has emerged as a key research area. Existing literature indicates that fully autonomous systems are rarely deployed without human supervision. Instead, AI systems function as decision-support tools, assisting operators rather than replacing them. Researchers argue that poorly designed user interfaces can lead to automation bias, over-reliance on AI recommendations, or complete distrust of system outputs. This highlights the need for user-centered design approaches that balance automation with meaningful human control.Several studies have proposed UX evaluation frameworks for AI-based systems, focusing on factors such as usability, trust, transparency, response time, and perceived system reliability.

Empirical evaluations using usability testing, surveys, and task-based experiments reveal that AI systems with intuitive interfaces and transparent feedback mechanisms result in better operator performance and faster decision making. However, most existing studies address UX evaluation in general AI applications such as healthcare, finance, and consumer technologies, with limited focus on defense-specific systems.Furthermore, research on AI-based defense systems often prioritizes technical performance metrics, such as detection accuracy and system efficiency, while UX considerations remain secondary. This creates a

research gap in systematically integrating UX design principles into AI based defense platforms. Recent studies emphasize the importance of human centered design and UX evaluation in mission-critical systems, advocating for multidisciplinary approaches that combine AI engineering, usability engineering, and cognitive psychology.In summary, existing literature establishes the effectiveness of AI in defense applications but reveals limitations related to usability, explainability, and human trust. There is a clear need for research that systematically addresses user experience design and evaluation in AI-based defense systems. This study builds upon prior work by proposing a UX-oriented framework tailored to defense environments and empirically evaluating its impact on operator performance, trust, and system effectiveness.

Author(s) & Year	Research Focus	Methodology Used	Key Findings	Research Gap Identified
Goodfellow et al. (2016)	Deep learning foundations	Deep learning foundations	Demonstrated high accuracy of deep learning models	Lacks focus on user interaction and usability
Shabtai et al. (2012)	Android malware detection	Behavioral analysis	Improved threat detection using ML	No consideration of user experience
McLaughlin et al. (2017)	AI-based malware detection	Deep learning models	Enhanced detection of complex threats	Explainability and UX not addressed
Choo (2011)	Cyber threat landscape	Analytical study	Identified evolving cyber threats	No UX or human–AI interaction focus
ENISA (2023)	AI cybersecurity challenges	Policy and risk analysis	Highlighted trust and transparency issues	Limited UX evaluation methods

III. Related Work

Research on intelligence defense systems is growing really fast. It is looking at things like finding threats making decisions on its own watching what is going on and defending against cyber attacks. At first people were trying to make the artificial intelligence better at doing things. They used machine learning and deep learning to make it work. These studies showed that artificial intelligence is really good at finding changing threats, much better than the old ways of doing things.. A lot of these studies did not think about the people using the artificial intelligence defense systems. They did not consider how the people would feel about using it or how easy it would be for them to use. The artificial intelligence defense systems need to be designed so that people can use them easily.

People who study how humans and computers work together have looked at how smart systems can be used in a way that's easy for people to understand. They think it is very important that these systems are simple to use do not confuse people and have interfaces that are well designed. When we look at things like airplanes and hospitals we see that if the interfaces are not designed well people are more likely to make mistakes and have a time understanding what is going on. This is also very important for defense systems, where people have to make sense of information that is generated by intelligence when they are under a lot of pressure and things are not clear. The human-computer interaction aspects are really important, in these defense systems because the people using them have to interpret the intelligence generated information under time pressure and uncertainty and this is a key part of human-computer interaction. There are not

studies that use Human Computer Interaction principles when they make AI systems for defense. Human Computer Interaction principles are not really used that much when people make AI systems for defense.

Explainable AI, which is also known as XAI is a deal when it comes to making AI systems more transparent and trustworthy. People have done a lot of research. Found out that when AI systems can explain their decisions in a way that makes sense users are more likely to trust them and feel confident about the choices they make. For example in defense-related applications people have used things, like feature visualization and confidence indicators to help operators understand what the system is recommending. They have also used rule based summaries to make things clearer.. Even with all these advances, the way XAI is used often does not work well with the overall design of the user experience. This can make it hard for users to interact with the system in a way. Explainable AI systems need to be designed in a way that takes into account the user experience.

People have been looking at how to figure out if AI systemsre easy to use. They want to know if people trust these systems and if they are happy with them. They also want to know if people think these systems are reliable. When we look at what people say about these systems we can see that systems that are designed with the user in mind work better and people like them more.. Most of the time these studies are not about systems used by the military. They are about systems used in places, like hospitals, banks and shops where people buy things. Defense situations are really tough. They have a lot of things that make them special like people having to think hard and make big decisions very quickly. The fact that these situations can be very risky is also a deal. Usually these things are not handled well. Defense environments have cognitive load, time-critical decisions and risk sensitivity that are often In the cybersecurity field people have looked at how defense tools that use Artificial Intelligence work with human analysts. Studies show that Artificial Intelligence helps find threats accurately but analysts have a hard time understanding what the system is telling them. This is because the systems are complicated and do not give information about what is going on. This problem shows that we need to make the systems easier to use so they work better for the analysts.. Most of the time people who make these systems focus on making the backend smarter instead of making it easier for the analysts to use the frontend. We are talking about Artificial Intelligence and cybersecurity here. We need to make sure the systems are helpful, for the analysts who use them and that is why we need to focus on Artificial Intelligence and cybersecurity systems that are easy to use.

Overall, the reviewed literature demonstrates significant progress in AI capabilities for defense systems but reveals a lack of holistic approaches that integrate AI performance with UX design and evaluation. Few studies provide structured frameworks that combine human-centered design, explainability, and usability evaluation specifically for AI-based defense systems. This research addresses this gap by presenting a comprehensive UX-oriented approach tailored to defense applications and empirically evaluating its impact on human–AI collaboration and system effectiveness.

IV. METHODOLOGY

This research adopts a human-centered methodology to design and evaluate the user experience (UX) of an AI-based defense system. The methodology integrates system design, UX development, and empirical evaluation to assess the effectiveness of human–AI interaction in defense environments. The overall workflow consists of requirement analysis, system architecture design, UX framework development, implementation, and evaluation.

1. Requirement Analysis The first phase involves identifying functional and user experience requirements of AI-based defense systems. Requirements are gathered through a review of existing defense systems, analysis of operator workflows, and evaluation of common usability challenges reported in literature. Key requirements include efficient threat visualization, system transparency, minimal cognitive load, fast response time, and high usability under time-critical conditions.

2. AI-Based Defense System Architecture The proposed defense system is designed using a modular architecture consisting of data acquisition, AI processing, decision support, and user interface layers. The AI module employs machine learning techniques for threat detection and risk assessment. The decision support

layer generates alerts and recommendations, which are communicated to users through an interactive interface designed to support rapid understanding and action.

3. UX Framework Design A human-centered UX framework is developed by incorporating principles from human–computer interaction (HCI), usability engineering, and explainable AI (XAI). The interface design focuses on clarity, consistency, and minimalism to reduce cognitive load. Explainability features such as confidence scores, visual indicators, and contextual explanations are integrated to improve transparency and user trust.

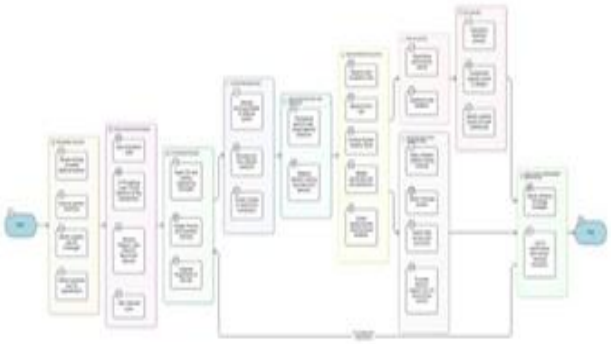
4. System Implementation The AI-based defense system and user interface are implemented using a prototype-based approach. The system simulates real-time defense scenarios to evaluate user interaction and decision-making behavior. Multiple interface versions are developed to compare UX design improvements and assess their impact on operator performance.

5. User Experience Evaluation He evaluation phase employs both quantitative and qualitative methods. A group of participants with technical backgrounds is selected to interact with the system in task-based scenarios. UX evaluation metrics include task completion time, error rate, System Usability Scale (SUS), perceived trust, and user satisfaction. Post-interaction questionnaires and structured feedback sessions are conducted to collect subjective user insights.

6. Data Analysis Collected data is analyzed for descriptive and comparative statistical purposes. Various performance parameters are compared for different designs to measure the enhancements made to the usability aspect. Feedback received is analyzed for general usability issues, user preference, or areas for future improvements.

7. Validation and Ethical Considerations In order to have the validity of the study intact, the evaluation procedure is conducted using standard usability testing methodologies. Human subjects issues such as informed consent, ensuring privacy of data, and the use of anonymous responses by users are observed. Only the usage decision-support capability is assessed with no human oversight allowed over the decision.

8. Summary of Methodological Workflow This proposed methodology ensures the review in a structured way the UX of AI-based defense systems, relating technical performance of AI with human-centered assessment, which identifies UX design strategies for improving usability, trust, and operational effectiveness.



Flow chart

V. USE OF CASE ARCHITECHTURE

User interaction with an AI-driven defense system, as well as the way in which system components work together in relation to support for threat detection and decision-making, can be described in use case architecture. Use case architecture is designed in such a way as to facilitate efficiency in human-AI team collaborations. Efficiency in human-AI collaboration is crucial in a high-threat defense context.

The main interaction occurs when the defense operator gains trusted access to the system through the authentication log-in process. Once authenticated, the defense system is continuously gathering data from a combination of sources both within and external to the defense system itself, such as sensors and monitoring sources. This data is then processed by the AI defense engine, which employs ML to analyze threats and provide alerts on the basis of predetermined levels of threat confidence.

The threats identified are relayed to the operator by means of a user-friendly interface that emphasizes priority notifications and ensures a clear understanding of system situations. To facilitate decision-making, the system has explainability capabilities that involve context and confidence information, which enable the operator to comprehend the reasoning for AI-driven advice.

Based on the system outputs, the operator analyzes the suggested actions to take and launches corresponding responses, for instance, acknowledging warnings, escalating incidents, or implementing mitigations. Human oversight is integrated throughout the process to provide accountability to cover the risks related to automation biases. On the whole, the case use architecture defines a structured flow of interaction where data acquisition, analysis by AI, visual analysis, explanation, and human decision-making are closely coupled.
The case use architecture improves usability, trust, and effectiveness of the AI powered defense system by incorporating user experience into each interaction. Human decision making is the core of the use case architecture.

The operators interpret and analyze the results of the AI-based alert and recommendation systems prior to triggering the responsive action. In turn, this limits the chances of automation bias and promotes accountability with the defense operation. The user inputs, responses, and feedback are measured to monitor performance and optimize the AI and UX design continuously.The use case architecture creates a continuous and user-friendly flow of interaction between data gathering, AI computation, data visualization, explanation, and human reaction. Through the systematic consideration of UX through every step of the architecture, the AI defense platform is rendered efficient through human – AI collaboration.

VI. Probable Outcomes

The proposed study shall be able to show, through its implementation, the practical effectiveness of applying user-centered design principles to AI-based defense systems. The primary aim of applying user centered principles to AI system interface design within this project shall help enhance the effectiveness of the AI system, as its interface can potentially help defense system operators understand insights gleaned by AI faster.

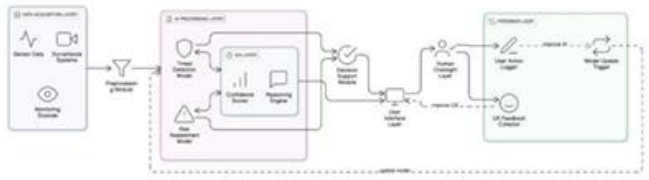
A further likely result of the research is that it will lead to increased user trust and confidence in AI based defense systems. This is because the incorporation of explainable AI components such as confidence indicators and contextual explanations will help alleviate uncertainties and mistrust of automated decision-support systems. Therefore, the users will be able to trust and leverage the recommendations of the AI systems while having effective control.

Furthermore, it is expected that the results of the evaluation will demonstrate measurable gains in usability metrics such as System Usability Scale scores, task completion time, and the rate of errors compared to traditional or unoptimized defense graphical user interface designs. Outcomes from the study will reveal the positive impact of user experience on human performance.

The research is also likely to point out the balancing of automation and human control in defense applications. By positioning AI as a supportive decision-making agent, rather than a fully autonomous system, the proposed approach might alleviate some automation bias and over-reliance risks on intelligent systems. This outcome reinforces the necessity of human–AI collaboration in safety critical environments.

The study is also supposed to provide concrete design guidelines and insights into usability evaluations that will be useful for the development of future AI-based defense systems. The resultant outcomes can help researchers, system designers, and defense practitioners in the development of reliable, trustworthy, and user-friendly AI-driven defense solutions, and also identify the directions for future research and system enhancements.

VII. IMPLICATIONS



The implications of the current research for the use of AI defense systems are very significant. In other words, the fact that the usability of the system and the performance of the operations executed by the system can be influenced through the use of user centered system design highlights that user experience is not something that should be treated as a minor factor. On the contrary, the use of defense systems that incorporate user experience could improve the situation awareness and the efficiency of decision-making.

In a practical sense, the proposed framework for a UX focus is useful for system designers and developers to effectively design AI defense systems that are robust as well as user-friendly. The incorporation of explainable AI functionality into the user interface is a significant step that can bridge the gap between human comprehension and complex AI systems. This can ensure effective collaboration between humans and AI while counteracting the risks posed by automation bias and incorrect interpretation of the system's output.

The findings of the research also imply a number of implications for practice related to defense organizations. Enhanced usability and transparency will help reduce the training process for new users. Concerning the research aspect, this work advances the existing body of knowledge regarding human-centric AI in terms of the significance of UX evaluation for safety-critical systems. It suggests further investigations in the area of interdiscipline for artificial intelligence research and human computer interaction with usability engineering. The findings of this work can be applied for the safety related domains like cybersecurity, healthcare, and transport systems.

In general, the implications of this research work suggest the need to develop AI defense systems with high performance capability as well as the ability to support successful interaction with humans.

VIII. REASERCH GAP

Current studies involving AI-based defense systems have mainly concerned algorithmic improvements, automation, and enhanced threat detection. While these works illustrate the technical efficiency of artificial intelligence in defense applications, they largely fail to consider the importance of UX in guaranteeing proper collaboration between humans and AI. This results in most AI-driven defense systems lacking usability, transparency, and interpretability very important aspects of high-risk and time-critical settings.

While human–computer interaction and usability engineering have been well studied in general AI applications, a limited amount of work has systematically applied these principles to defense-specific systems. Nearly all the existing UX evaluation frameworks are designed to suit domains such as healthcare, finance, or consumer applications and fail to fully consider the specific operational constraints of the defense environment: high cognitive workload, rapid decision making, and continuous situational awareness.

Research in explainable AI has also shown its potential to enhance trust and understand decisions made by AI; however, the incorporation of explainability features into overall UX design frameworks for defense systems remains inadequate. Most research studies explainability consider as one isolated technical feature

without embedding it into user workflows and interface design. Consequently, fragmented user interactions occur that do not fully support operator decision-making.

Another significant gap that has been observed is that there is a lack of empirical studies that examine both system performance measures and usability measures in Artificial Intelligence-based defense systems. Current studies that work on assessing these systems mostly consider metrics like detection accuracy and response times rather than metrics related to usability and associated user trust and mental workload.

Hence, there lies a research gap in the design and study of defense systems that specifically implement artificial intelligence solutions in terms of human-centered UX design, explainability in AI, and usability studies. In this study, the proposed research aims to fill the said gap through the formulation of a structured approach related to UX design with empirical verification of its effects.

IX. CONCLUSION

This paper offered a human-centric perspective on the design and assessment of the user experience of a defense system based on AI. Although AI has greatly advanced the technical capabilities of contemporary defense systems, this work illustrates the important aspects of the quality of the process of interacting with AI systems for the effectiveness of the defense system itself. By incorporating the aspects of the user experience into the system design process, the suggested model facilitates better collaboration of the human with the AI system.The results show the effectiveness of the incorporation of usability engineering concepts and the use of explainable AI systems in the defense system interface for achieving a better understanding of the system and a more efficient decision-making process. The results of the assessments indicate the effectiveness of human-centric system design for achieving usability and enhancing the system acceptance Moreover, this paper fills an existing gap in the literature by not only emphasizing the use of AI in a defense scenario but also providing a framework that properly blends AI capability with UX design. This is a significant contribution to existing literature and knowledge in this field.

In conclusion, it is pertinent to note that the study highlights the significance of a harmonious convergence of AI technologies and human-centric design aspects if AI based defense systems are to be successfully implemented. It has been suggested that for future defense technologies, user-centricity, along with a focus on AI algorithms, be made a priority.

X. REFRENCES

[1] M. A. Siam et al., “AI-Driven Cyber Threat Intelligence Systems: A National Framework for Proactive Defense Against Evolving Digital Warfare,” International Journal of Computational and Experimental Science and Engineering (IJCESEN), vol. 11, no. 3, pp. 6126–6140, 2025, doi: 10.22399/ijcesen.3793.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2]

[3] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.K. Elissa, “Title of paper if known,” unpublished.

[4] A. Shabtai, U. Kanonov, Y. Elovici, C. Glezer, and Y. Weiss, “Andromaly: A Behavioral Malware Detection Framework for Android Devices,” Journal of Intelligent Informtion Systems, vol. 38, no. 1, pp. 161–190, 2012.

[5] W. Stallings, Cryptography and Network Security: Principles and Practice, 8th ed. Pearson Education, 2023.

[6] M. Conti, T. Dargahi, A. Dehghantanha, and N. K. Giannetsos, “A Survey on Man-in-the-Middle Attacks,” IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2027–2051, 2016.

[7] N. McLaughlin et al., "Deep Android Malware Detection," in Proceedings of the 7th ACM Workshop on Artificial Intelligence and Security, 2017, pp. 1 11.

[8] ENISA, Artificial Intelligence Cybersecurity Challenges, European Union Agency for Cybersecurity, 2023.

[9] S. Vinayakumar, K. P. Soman, and P. Poornachandran, "Applying Deep Learning Approaches for Network Traffic Prediction," International Journal of Advanced Research in Computer Science, vol. 8, no. 5, pp. 235–240, 2017.

[10] K. R. Choo, "The Cyber Threat Landscape: Challenges and Future Research Directions," Computers & Security, vol. 30, no. 8, pp. 719–731, 2011.

[11] P. K. Sharma and J. H. Park, "Blockchain-based Hybrid Network Architecture for Secure IoT," Future Generation Computer Systems, vol. 99, pp. 688–696, 2019.