Leveraging ai-driven requirements for sysml modeling of the iobt: A comprehensive investigation

Joseph J. Brooks, *Middle Georgia State University, Joseph.Brooks2@mga.edu*

Abstract

It can be challenging to determine system requirements and model systems for the Internet of Battlefield Things devices that must function in various highly demanding circumstances, especially considering all the potential problems these devices could encounter. To support military organizations, there needs to be a means to take advantage of AI/ML's capabilities to help appropriately and expeditiously derive secure requirements that enable efficient modeling of these systems. The application of a framework for requirements derivation and model-based systems engineering for Internet of Battlefield Things (IoBT) devices was examined in this literature review. This research investigates the Large Language Model's capabilities to enhance the model-based systems engineering process.

Keywords: MBSE, LLM, Generative AI, requirements engineering, SysML, IoBT

Introduction

The Internet of Things (IoT) has emerged as a transformative force in both civilian and military domains, with projections indicating that by 2025, approximately 21.5 billion IoT devices will be connected to the Internet, generating an estimated $11.1 trillion in revenue (Langleite et al., 2021). The widespread adoption of IoT is driven by its low development costs, ease of connectivity, and operational efficiency, leading to strategic adoption by military organizations to enhance battlefield capabilities. For instance, the effectiveness of drones in modern warfare has been well documented, particularly in the Ukraine conflict, where drones have enabled cost-effective, precision strikes through direct engagement or artillery guidance (Barbu, 2024). Recognizing this growing dependence on unmanned systems, former U.S. Defense Secretary Lloyd Austin emphasized that the outcome of future conflicts may largely depend on drone warfare, leading to a classified counter-drone strategy aimed at mitigating threats posed by adversarial IoT-enabled military assets (McIntyre, 2024). The Internet of Battlefield Things (IoBT) has significantly reshaped military operations, enhancing intelligence gathering, battlefield communications, and strategic decision-making. However, securing interconnected IoT military devices against sophisticated cyber threats remains a formidable challenge. Conventional security mechanisms, such as encryption, intrusion detection, and secure communication protocols, have been extensively researched. However, the rapid expansion of IoT networks has exacerbated vulnerabilities in data security and infrastructure integrity (Alaba et al., 2020; Stocchero et al., 2023). Cybercriminals increasingly exploit zero-day vulnerabilities by deploying attacks such as GPS spoofing, botnet attacks, and signal jamming to compromise military IoT systems, underscoring the urgent need for innovative security solutions (Adel & Jan, 2024; Toth, 2021).

Despite growing research on AI in cybersecurity, particularly in threat detection and anomaly analysis, limited studies have explored AI-driven automation for security requirements engineering in IoBT systems (Alkhabbas et al., 2016). Traditional approaches to security requirement derivation are labor-intensive and error-prone, and they struggle to keep pace with the evolving cyber threat landscape, leaving military systems vulnerable to exploitation (Adel & Jan, 2024). AI-based automation, mainly through Large Language Models (LLMs) such as ChatGPT, presents a promising solution to streamline security requirements extraction, enhance precision, and increase scalability in military IoT security design. However, AI's role in automating the derivation of structured and formalized security requirements for IoBT remains underexplored. This study conducts a systematic literature review to analyze existing approaches, future research trends, and gaps in AI-driven automation for security requirements engineering, particularly in SysML and LLMs for IoBT device security. By synthesizing findings from prior research, this study aims to provide scholars and practitioners with a comprehensive understanding of how AI can automate security requirements engineering, thereby improving efficiency, mitigating cybersecurity risks, and adapting to evolving regulatory frameworks (Langleite et al., 2021; Rosenberg et al., 2024). Addressing

these research gaps is essential to developing scalable, AI-assisted security frameworks that can enhance the resilience and adaptability of IoBT security architectures for modern military applications.

Problem Statement

The rapidly changing dynamics of contemporary battlefields necessitate sophisticated and adaptable technical solutions to improve operating efficiency and situational awareness (Stocchero et al., 2023). The Internet of Battlefield Things (IoBT) has become essential in contemporary defense operations, requiring exact and adaptable security measures to guarantee the robustness of these interconnected systems. However, traditional requirements engineering and system modeling methodologies are insufficient in adapting to the rapidly evolving nature of warfare, resulting in delays, inconsistencies, and possible security risks in IoBT development. Large Language Models (LLMs), such as ChatGPT provide a viable solution by analyzing natural language inputs and dynamically creating security and functional requirements in real-time (Alaba et al., 2017). Notwithstanding this potential, incorporating AI-generated requirements into Model-Based Systems Engineering (MBSE) tools like SysML poses considerable obstacles. AI-generated requirements frequently lack the structural rigor, traceability, and formal syntax essential for direct implementation in SysML models, leading to errors, misalignment, and increased verification overhead. The lack of defined procedures for AI-driven requirement formulation and validation creates problems regarding accuracy, completeness, and adherence to military security guidelines. Closing the divide between AI-assisted requirement engineering and SysML modeling is essential for improving the security, efficiency, and adaptability of IoBT systems (Apvrille & Sultan, 2024). This study examines the current literature on AI-driven automation of security requirements, emphasizing existing constraints, obstacles, and possible solutions to facilitate the smooth and dependable incorporation of AI-generated requirements into Model-Based Systems Engineering frameworks for the Internet of Battlefield Things.

Purpose of the Study

This research addresses a critical gap in AI-driven security requirements engineering by exploring the effective integration of Systems Modeling Language (SysML) and advanced artificial intelligence (AI) to formulate comprehensive security requirements for Internet of Battlefield Things (IoBT) devices. Current approaches for generating security requirements frequently depend on laborious, manual processes that fail to adapt to contemporary military operations' dynamic and evolving characteristics. This study examines the potential of ChatGPT's natural language processing (NLP) capabilities to automate and improve the accuracy, efficiency, and adaptability of security requirement derivation in Model-Based Systems Engineering (MBSE) frameworks. This work seeks to reconcile AI-generated security needs with formal SysML modeling by methodically analyzing existing research, assuring that requirements are organized, traceable, and compliant with military cybersecurity standards. This research's findings have substantial implications for military and systems engineering, as AI-driven automation can boost threat modeling, minimize human error, expedite deployment processes, and bolster the robustness of IoBT systems against cyber threats. This research illustrates the synergistic potential of AI and SysML, offering a scalable framework applicable to future military IoT applications and enhancing the development of secure, adaptive, and intelligent battlefield systems.

Research Question

R.Q.1: What are the existing approaches and challenges in integrating Systems Modeling Language (SysML) and Large Language Models (LLMs) to automate the derivation of secure system requirements for Internet of Battlefield Things (IoBT) devices?

R.Q.2: How can AI-driven tools such as ChatGPT be integrated with MBSE methodologies to automate the derivation of security requirements for IoBT devices?"

Review of the Literature

The Evolution and Importance of IoBT in Military Operations

The convergence of Internet of Things (IoT) technology with military applications has given rise to the Internet of Battlefield Things (IoBT) (Apostolopoulos, 2022). Kafakunesu et al. (2025) asserted that this technology is revolutionizing contemporary warfare through the interconnection of diverse equipment and

systems vital for battlefield operations. This connectivity enables real-time or near real-time communication, data sharing, and collaboration across military assets, improving situational awareness, decision-making, and overall operational efficacy. IoBT can be seen as an interconnected ecosystem of sensors, autonomous devices, and battlefield communication systems, enabling real-time or near real-time intelligence gathering, troop coordination, and enhanced operational effectiveness. Studies emphasize that IoBT devices operate in dynamic and contested environments, requiring robust, adaptive, and secure architectures to withstand adversarial threats (Feng et al., 2020). IoBT networks rely on Low Powered Wide Area Networks (LPWAN), Wireless Sensor Networks (WSN), Mobile Ad-hoc Networks (MANETs), and Flying Ad-hoc Networks (FANETs) to facilitate data transmission and decision-making across military units (Kang et al., 2020; Ma et al., 2020). However, the increasing complexity of these networks introduces significant cybersecurity challenges, making security-driven requirements engineering essential for developing and deploying IoBT systems (Alaba et al., 2020). Furthermore, while the Department of Homeland Security (2016) recommends security integration during the design phase, military IoBT systems often lack the means to make this process less laborious by integrating automated tools that can assist in security requirements derivation, leading to decreased vulnerability to emerging cyber threats.

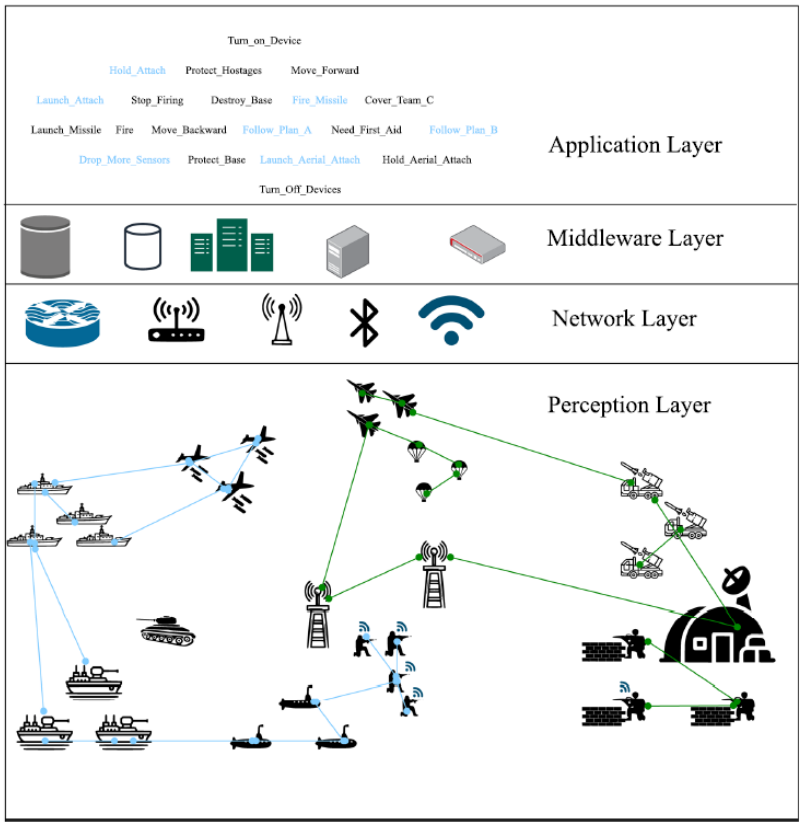
Security Vulnerabilities and Threats in IoBT Systems

IoBT systems encompass a diverse range of unmanned and autonomous military technologies, including Unmanned Aerial Vehicles (UAVs), Unmanned Ground Vehicles (UGVs), Unmanned Surface Vehicles (USVs), Unmanned Underwater Vehicles (UUVs), military wearables, and satellite-based communication systems (Werbinska-Wojciechowska et al., 2024). However, these systems face numerous attack vectors, requiring rigorous security engineering methodologies. UAVs, a critical component of modern warfare, are vulnerable to jamming, spoofing, and cyber-hijacking (Adel & Jan, 2024). Similarly, while enhancing situational awareness and medical monitoring, military wearables face risks from data breaches due to limited computational power and physical tampering (Perez & Zeadally, 2021). Furthermore, adaptive communication protocols in UAV FANETs have improved battlefield coordination, but they also increase susceptibility to denial-of-service (DoS) and latency-related attacks (Zheng et al., 2024).

Emerging Threats in IoBT Communication Protocols

Emerging threats in the Internet of Battlefield Things (IoBT) communications present significant challenges to ensuring secure, resilient, and efficient data exchange in military environments. As IoBT networks grow increasingly complex, with diverse, battery-powered devices like sensors, UAVs, and wearables, they face vulnerabilities to cyberattacks such as jamming, eavesdropping, and data manipulation (Kafakunesu et al., 2025). Low-latency communication is essential for real-time operations. However, network congestion, malicious interference, and scaling issues, especially when thousands of devices are deployed simultaneously, heighten the risk of packet loss, degraded performance, and compromised mission effectiveness (Nomikos et al., 2024). Furthermore, energy-efficient protocols are critical to extending device operation in environments where frequent recharging is unfeasible (Kafakunesu et al., 2025). The shift to 6G-enabled UAV swarms in maritime warfare further amplifies the need for secure, high-reliability communication protocols to counter emerging cyber threats (Nomikos et al., 2024). Innovative solutions, including AI/ML-based threat detection, blockchain, and advanced encryption protocols, are being explored to address these vulnerabilities and ensure robust IoBT communications in future battlefield scenarios (Kafakunesu et al., 2025).

Figure 1
Layers of IoBT architecture (Kafakunesu et al., 2025)



Challenges in Requirements Engineering for IoBT Security
Requirements Engineering (RE) is a structured methodology to identify, analyze, and validate security constraints in the IoBT systems (Aguilar-Calderon et al., 2022). Traditional manual RE processes, however, face challenges in keeping up with rapidly evolving cyber threats and adversarial tactics, particularly in military settings. Studies have pointed out several limitations of conventional RE approaches, including inconsistent threat modeling, scalability issues, and slow responses to emerging vulnerabilities (Alaba et al., 2020; Singh et al., 2020). To address these issues, Kamalrudin et al. (2017) advocate for a sociotechnical approach to IoBT security requirements, highlighting the importance of human-AI collaboration for adaptive threat modeling. Additionally, Ahmad et al. (2022) emphasize the potential of AI-driven methodologies to improve security requirements' efficiency, completeness, and traceability, underscoring the growing need for automated approaches in IoBT system development.

Machine Learning & Natural Language Processing (NLP) in Security Requirements
LLMs, such as ChatGPT, can process unstructured threat intelligence data and derive contextually relevant security requirements (Shaukat et al., 2020; Marques et al., 2024). Rosenberg et al. (2024) describe how LLMs interpret prompts, which involves several steps. Initially, the input text is broken into smaller units called tokens, each converted into a numerical value. These values are then passed through an embedding layer that transforms them into continuous vector representations, capturing both the meaning of each token and its relationship to others. Based on these embeddings, the model generates a response. Phojanamongkolkij et al. (2023) posit how AI-driven knowledge graphs can automate requirement discovery, reducing human error in security specifications. Despite these advancements, a significant challenge remains in translating AI-derived requirements into structured modeling languages, such as SysML, without introducing inconsistencies (Blasek et al., 2023).

AI and SysML in Automating Security Requirements Engineering

Integrating Artificial Intelligence (AI) with requirements engineering has transformed the automation of system specification derivation, refinement, and validation, particularly in MBSE. One of the most notable advancements is the automated generation of Systems Modeling Language (SysML) diagrams from textual system specifications, enabling a seamless transition from high-level requirements to structured model representations (Apvrille & Sultan, 2024). Automating requirements into SysML diagrams has evolved through advancements in Natural Language Processing (NLP) and domain ontology techniques, significantly improving requirement extraction, system modeling, and consistency validation. NLP-based methodologies and tools, such as the Requirement Analysis to Provide Instant Diagrams (RAPID) tool, enabled automated concept extraction, syntactic reconstruction, and Unified Modeling Language (UML) (the SysML precursor) diagram generation from textual specifications (More & Phalnikar, 2012). These processes rely on two essential inputs: the system specification and an inquiry that guides the AI in extracting relevant information and generating appropriate SysML representations. To ensure model consistency and coherence, existing SysML diagrams can be used as supplementary inputs, allowing AI to cross-reference past models while generating new ones. To enhance accuracy, the AI translation process also leverages domain-specific knowledge, including diagram formatting conventions, semantic constraints, and structural principles (Delligatti, 2014). LLMs comparable to ChatGPT enable AI to process structured inputs and output results in formats like JSON, XML, or SysML textual syntax, facilitating direct integration with MBSE tools like TTool (Rosenberg et al., 2024). By bridging AI-powered natural language processing (NLP) with SysML-based security modeling, AI-driven automation offers a scalable alternative to traditional manual requirement engineering methods.

Despite its advantages, LLMs' inherent randomness introduces challenges in ensuring accuracy, relevance, and consistency in AI-generated SysML models. To address this, automatic feedback loops iteratively refine AI-generated content, improving alignment with structured system requirements before final approval and diagram generation (Apvrille & Sultan, 2024). Beyond SysML translation, AI enhances security requirement engineering in high-risk domains such as the IoBT, where real-time threat intelligence analysis and adaptive security requirement formulation are essential. AI-driven iterative techniques, such as the zigzag and deep-dive strategies, further improve security requirements by refining contextual accuracy through interactive prompting (Rosenberg et al., 2024). These methodologies ensure dynamic security requirement generation and adaptability to emerging cyber threats (Langleite et al., 2021). Furthermore, AI-assisted security engineering fosters compliance with cybersecurity standards, such as NIST recommendations structuring security objectives into traceable, actionable requirements (Rosenberg et al., 2024). By integrating AI-driven security requirement derivation with SysML automation, this research provides a unified, scalable framework for contemporary requirements engineering, promoting traceability, adaptability, and compliance in modern cyber-physical and military defense systems (Apvrille & Sultan, 2024; Rosenberg et al., 2024).

Figure 2

Traditional vs. AI-Driven Security Automation Methodologies

Aspect	Traditional Security Automation	AI-Driven Security Automation
Requirement Extraction	Involves labor-intensive, time-consuming activity that is highly susceptible to human error	Automated extraction from cybersecurity policies and threat intelligence
Processing Speed	Slow processing that requires extensive human validation	Real-time processing and validation
Adaptability to Evolving Threats	Involves reactive adaptability which requires manual updates	Proactive adaptability that dynamically adapts to evolving threats

Human Involvement	High human involvement is needed which necessitates human analysts reviewing and adjusting policies	Minimal human involvement is needed due to AI automating updates and refining security requirements
Error Rate	Higher risk of inconsistencies and omissions	Reduced human error equates to enhanced accuracy, and consistency
Traceability & Compliance	Requires manual documentation and auditing	AI-enabled traceability and compliance verification reduces a significant amount of manual work needed
Scalability	Limited scalability across complex military networks	Highly scalable for large IoBT deployments
Threat Detection and Response	Delayed response to emerging threats, requiring manual intervention	Real-time anomaly detection and automated threat response

Research Gap

Despite significant advancements in AI-driven security requirement automation for the IoBT, several critical areas remain underexplored or partially addressed. One of the most prominent gaps is the lack of standardized frameworks for integrating AI-generated security requirements into MBSE tools, such as SysML. While existing research has explored AI's role in threat detection, anomaly analysis, and security automation, it is not readily apparent within the literature what has been done to establish bidirectional traceability mechanisms that ensure AI-derived security policies remain consistent, adaptable, and verifiable within structured system models (Apvrille & Sultan, 2024; Rosenberg et al., 2024). While LLMs similar to ChatGPT have demonstrated potential in extracting security requirements, their contextual accuracy, domain-specific applicability, and real-time adaptability for IoBT security engineering remain underdeveloped. The literature has yet to fully address how AI-driven security adaptation models can dynamically adjust security requirements in response to evolving cyber threats, ensuring continuous compliance with military-grade security standards (Langleite et al., 2021; Adel & Jan, 2024). Furthermore, there is limited empirical validation of AI-SysML integration in real-world military IoT environments, making it challenging to assess AI-driven security engineering solutions' scalability, effectiveness, and interoperability (Alaba et al., 2020).

Methodology

The employed approach is a systematic literature review, using the principles established by Barbara Kitchenham and conforming to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines. This study comprises three phases: 1. Planning the review, 2. Conducting the review, and 3. Reporting the review. This structure ensured a systematic and comprehensive examination of the research concerning using an LLM to derive system requirements for IoBT devices. This systematic literature review (SLR) followed the guidelines established by Kitchenham and Charters (2007). Defined inclusion and exclusion criteria limit this study. The criteria for inclusion are Peer-reviewed journal articles, conference papers, technical reports, and reputable industry white papers addressing security aspects related to cybersecurity, threat modeling, or secure system design in the context of IoT/IoBT systems. This paper utilizes studies published within the last two decades of exploration, with a preference for those addressing recent advancements in integrating AI and MBSE. The exclusion criteria encompass papers that discuss MBSE or SysML without mentioning Artificial Intelligence, Machine Learning, or LLMs. Papers that overlook secure system requirements and focus solely on performance optimization, cost reduction, or general automation issues will be excluded from the final selection of papers. Papers employing outdated methods, pre-SysML v2.0, legacy AI models that do not align with current AI advancements, and articles that provide only conceptual discussions without practical case studies, implementations, or feasibility analyses will also be excluded.

The selection of pertinent studies is categorized into two phases. The initial phase involves selecting studies that meet the established inclusion and exclusion criteria. This was accomplished through an examination

of the papers' titles and abstracts. The second part involves selecting the final papers from the initially chosen list, contingent upon their adherence to the quality assessment criteria. The papers were read in their entirety to assess their relevance to this work. Articles were categorized within the reference manager software tool MENDELEY and analyzed across various topics. Elements were examined for overlap, and gaps were identified by reviewing each article's results, limitations, and proposed future research. A Microsoft spreadsheet was then used as a structured table providing an overview of individual and combined studies on integrating LLMs into the secure system requirements derivation process. This study does not claim the inclusion of all existing literature. However, it seeks to analyze research within designated categories to establish a basis for future inquiries into applying LLMs to generate secure system requirements for IoBT devices.

Table 1

Search Strings and Library Sources

Sources	Search String
GALILEO	("MBSE" OR "Model-Based Systems Engineering") AND ("AI" OR "Artificial Intelligence" OR "LLM" OR "ChatGPT") AND ("requirements engineering" OR "system architecture") AND ("SysML" OR "model-driven development") AND ("security constraints" OR "secure design patterns")
Google Scholar	(("MBSE" OR "Model-Based Systems Engineering") AND ("AI" OR "Artificial Intelligence" OR "LLM" OR "Large Language Model" OR "ChatGPT" OR "Generative AI" OR "NLP-based systems") AND ("requirements engineering" OR "system architecture" OR "requirement automation" OR "automated requirement derivation") AND ("SysML" OR "Systems Modeling Language" OR "model-driven development") AND ("security constraints" OR "secure design patterns" OR "cybersecurity constraints")) AND (("IoBT" OR "Internet of Military Things" OR "military systems" OR "defense applications") AND ("feasibility study" OR "challenges" OR "limitations"))
Wiley Online Library	"MBSE" anywhere and "ChatGPT" anywhere, and "Requirements" anywhere
INCOSE Library	MBSE AND CHATGPT AND Requirements

Analysis of Data

The information collected underwent systematic examination through theme analysis to identify repeating trends, technical innovations, and research deficiencies. Prominent issues encompassed AI-driven automation in requirements engineering, AI-SysML integration, risks related to cybersecurity in IoBT systems, and challenges related to bidirectional traceability. Emerging patterns in the literature indicated prevalent security vulnerabilities across diverse IoBT applications, highlighting the necessity for real-time or near-real-time adaptive security measures. Moreover, numerous studies robustly endorsed AI's potential function in automating the derivation and validation of security requirements.

This study's results directly respond to both research questions by illustrating how AI-driven security automation improves efficiency, accuracy, and adaptability in IoBT cybersecurity while highlighting significant challenges in AI-SysML integration. In addressing the initial research question, "How can AI enhance security requirement generation for IoBT systems?" the findings indicate that AI-driven models markedly decrease human error, automate the derivation of security policies, and improve traceability within structured MBSE frameworks (Apvrille & Sultan, 2024; Rosenberg et al., 2024). Artificial Intelligence-driven Natural Language Processing and Machine Learning methodologies enhance threat detection, validate security compliance, and facilitate real-time adaptability, ensuring dynamic updates to the Internet of Battlefield Things security frameworks. Addressing the second research question, "What are

the challenges and limitations in integrating AI-generated security requirements with MBSE using SysML?" the study identifies the absence of standardized frameworks for AI-SysML integration. This deficiency obstructs bidirectional traceability, structured validation, and the seamless adaptation of AI-driven security measures. AI can automate the generation of security requirements; however, the outputs necessitate expert validation and structured translation mechanisms to ensure alignment with SysML-based MBSE models. The study uncovers the necessity for domain-specific AI training datasets and real-time validation in operational military settings to guarantee compliance, effectiveness, and reliability in AI-driven security engineering. The findings underscore the necessity of standardizing AI-SysML security models, creating real-time AI-driven security adaptation frameworks, and integrating AI-generated security requirements with structured MBSE methodologies to enhance IoBT cybersecurity resilience and ensure compliance with military defense systems.

Table 2
ChatGPT Prompts for validation

#	ChatGPT IoBT System Prompts
1	"What are the domain objects for the Internet of Battlefield Things (IoBT) system? List them briefly, describing each object and its role in the system."
2	"Write a set of use cases for the IoBT system and analyze them to extract additional domain objects. Provide a table summarizing the use cases and the derived domain objects with descriptions."
3	"Describe the top-level components within each subsystem of the IoBT system. Present the information in a structured format, such as a list or table, highlighting the relationships and functionalities of each component."
5	"Describe the requirements for each subsystem in the IoBT system. Organize the requirements into separate tables for each subsystem, with columns for requirement name and description."
6	"List the software components needed for the IoBT system. For each software component, provide a detailed set of requirements."
7	"List and describe the database requirements for the IoBT system. Include data storage, access control, performance, redundancy, and compliance considerations. Organize the requirements into a structured list or table."
8	"List all security requirements to protect the IoBT system, its subsystems, and software components against all known cyber-attacks. Present the requirements in a table format with columns for requirement number, name, and detailed description."
9	"Export the security requirements into a SysML Requirements diagram, Export all of the top-level components into a SysML block definition diagram, and then create Internal Block Diagrams for all of the subsystems of the top-level components and then establish trace relationships between each component and the requirements that it satisfies as a SysML traceability matrix."

Results

This study shows how AI-driven security automation improves IoBT cybersecurity efficiency, accuracy, and flexibility while identifying AI-SysML integration issues. Through analysis, it was found that in response to the first research question, “How can AI improve security requirement generation for IoBT systems?" AI-driven models reduce human error, automate security policy derivation, and improve traceability within structured MBSE frameworks. AI-powered NLP and ML increase threat identification, security compliance validation, and real-time adaptability, ensuring dynamic IoBT security framework updates. While exploring the second research question, “What are the challenges and limitations in integrating AI-generated security requirements with MBSE using SysML?”, the study finds that the lack of

standardized frameworks for AI-SysML integration hinders bidirectional traceability, structured validation, and seamless AI-driven security adaptation. Automated security requirement creation by AI requires expert evaluation and structured translation to match SysML-based MBSE models. The paper recommends domain-specific AI training datasets and live validation in real military contexts to assure AI-driven security engineering compliance, efficacy, and dependability.

The results further demonstrate that contemporary AI models lack clearly defined frameworks for integration with SysML and MBSE tools, complicating their deployment. Moreover, security vulnerabilities in unmanned vehicles, communication networks, and military wearables persist as substantial difficulties, highlighting the necessity for developing AI-generated security models. Although AI-driven automation enhances the precision of security requirements by minimizing human errors and improving consistency, the scalability and adaptability of AI models are hindered by the lack of comprehensive AI-SysML integration frameworks, restricting their capacity to respond in real-time or near real-time to emerging threats. Moreover, while AI models can facilitate the automation of security policy formulation, professional evaluation, and testing, mechanisms must be in place to guarantee adherence to rigorous military cybersecurity standards. To provide compliance, auditability, and system integrity, AI-driven security models must be traceable within SysML frameworks. To reliably comprehend security standards, identify threats, and automate safe system designs, AI models must be trained on domain-specific, military-grade datasets that precisely represent the distinct problems and requirements of IoBT systems.

Framework for Creating Secure System Requirements

The study's findings emphasize the creation of a systematic framework for utilizing Large Language Models (LLMs) to automate secure system requirements for IoBT devices, guaranteeing precision, compliance, and flexibility in military cybersecurity. This framework initiates data collecting and preparation, utilizing military-specific datasets, threat intelligence reports, and operational limitations to train AI models while reducing bias. AI-driven security requirement generation utilizes Natural Language Processing (NLP) techniques to extract and categorize security regulations, guaranteeing structured and contextually relevant outputs. The framework uses SysML modeling techniques to connect AI-generated security requirements with MBSE, facilitating standardized translation mechanisms and bidirectional traceability for security compliance. The findings underscore the significance of validation and compliance enforcement, wherein human-in-the-loop (HITL) validation, regulatory mapping (NIST, DoD, NATO), and AI-assisted consistency checks guarantee that security policies adhere to military-grade standards. Moreover, real-time flexibility and ongoing learning mechanisms enable AI to observe emerging threats, dynamically adjust security requirements, and enhance security policies through iterative feedback loops. The platform prioritizes seamless deployment and execution by incorporating AI-validated security models into IoBT networks, UAVs, autonomous battlefield sensors, and military command systems, while automated compliance monitoring and resilience testing guarantee practical application. The findings underscore that AI-driven automation improves the efficiency and precision of security requirement engineering; however, challenges persist in standardizing AI-SysML integration and attaining real-time adaptability, necessitating continued research in domain-specific AI training and the standardization of cybersecurity automation.

Discussion of Findings

This study verifies that AI-driven automation of security requirements markedly improves accuracy, efficiency, and adaptability within cybersecurity frameworks for Internet of Battlefield Things (IoBT) systems. These results correspond with Apvrille & Sultan (2024), who illustrated that AI-driven security requirement extraction and modeling diminish human error, enhance compliance validation, and automate refining security policies in military cybersecurity systems. Ahmad et al. (2022) determined that AI's capacity to analyze natural language descriptions and formulate security policies enhances requirement engineering; nonetheless, expert validation is essential for adherence to military-grade cybersecurity standards. However, despite its benefits, this study supports Blasek et al. (2023) in revealing that AI-generated security requirements frequently exhibit insufficiently structured traceability within Model-Based Systems Engineering (MBSE) frameworks, especially in SysML-based architectures, thereby constraining their applicability for military system designers.

A principal discovery from this research is the imperative for real-time adaptability in AI-driven security frameworks to combat evolving cyber threats. Nomikos et al. (2024) assert that static security policies are inadequate in military cybersecurity because of the swiftly changing landscape of battlefield threats. This reinforces this study's focus on integrating AI with real-time threat intelligence analysis to facilitate proactive security updates instead of reactive ones. Furthermore, our results extend the work of Shaukat et al. (2020), who revealed that AI-based security models are susceptible to adversarial assaults, including data poisoning, deceptive strategies, and model manipulation. This paper builds upon previous research by emphasizing the necessity of anomaly detection, adversarial defensive strategies, and automated threat modeling to guarantee AI-driven cybersecurity resilience in IoBT networks. Adel & Jan (2024) expound upon these risks by outlining the vulnerabilities of unmanned aerial vehicle (UAV) communication networks, asserting that AI-driven security automation must integrate robust authentication and intrusion detection systems to safeguard military assets from cyber exploitation.

The study's results corroborate Rosenberg et al. (2024), who asserted that AI-generated security policies must be traceable and auditable within SysML-based MBSE workflows to ensure compliance and regulatory conformance. The absence of bidirectional traceability mechanisms highlighted in this study corroborates Aguilar-Calderon et al. (2022), who illustrated that successful AI-driven requirements engineering relies on the capacity to trace security policies from overarching regulations to detailed system implementations. This study corroborates Toth (2021), who emphasized the necessity for AI-driven security compliance verification frameworks to conform to international military cybersecurity requirements, including NATO guidelines and the U.S. Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC) framework. Stocchero et al. (2023) further substantiate this viewpoint by asserting that safe command and control for IoBT networks must be integrated into AI-driven security automation frameworks to provide mission-critical resilience against cyberattacks.

This research complements the existing knowledge on AI-SysML integration in military cybersecurity by illustrating how AI-driven automation of security requirements improves compliance, traceability, and adaptability in IoBT systems. This paper offers empirical insights into AI's limitations, complications, and practical applications in automating security engineering, building on past research that has identified its potential. The findings confirm that AI-driven security automation effectively minimizes errors, enhances compliance, and facilitates real-time flexibility. Nonetheless, as prior research has indicated, the standardization, validation, and enhancement of AI adversarial defenses require further advancement to guarantee that AI-generated security models are robust, durable, and prepared for operational deployment. Subsequent studies must enhance these findings by optimizing AI-driven security automation frameworks that flexibly respond to cyber-attacks while maintaining regulatory compliance in international military operations (Ahmad et al., 2022; Apvrille & Sultan, 2024; Rosenberg et al., 2024)

Table 3

Key Thematic Findings of the Systematic Literature Review

Thematic Finding	Key Insights
AI-driven security automation enhances accuracy	Artificial intelligence mitigates human error in the creation and assessment of security requirements.
Challenges in AI-SysML integration	Lack of standardized AI-SysML frameworks hinders seamless integration
Real-time adaptability of AI in cybersecurity	AI systems must continuously revise security policies in real-time.
Need for standardized AI-driven security frameworks	Security automation models necessitate standards for efficient deployment.
Bidirectional traceability for compliance	Imperative to ensure AI-generated security policies are traceable across system layers
AI-driven threat detection and response	AI models must detect, classify, and respond to emerging cyber threats

Military-grade ai training and validation	AI systems require specialized military-grade training datasets for effectiveness

Limitations of the Study

While this systematic literature review provides valuable insights into AI-driven security requirement automation for IoBT systems, several limitations must be acknowledged to contextualize the findings and guide future research. First, the study relies primarily on secondary data sources, including published military cybersecurity policies, AI-SysML integration models, and prior case studies. Due to the classified nature of military operations, certain proprietary or restricted datasets were inaccessible, limiting the ability to validate AI-driven security models against real-world cyber threats (Apvrille & Sultan, 2024). This constraint may have impacted the accuracy of AI-derived security requirements, as training datasets were constructed using publicly available information rather than classified operational data. Additionally, the rapid evolution of AI and cybersecurity technologies presents a challenge in ensuring the long-term applicability of this research. AI models, including LLMs such as ChatGPT, undergo continuous advancements, and newer, more efficient architectures may surpass the methods explored in this study (Rosenberg et al., 2024). As a result, the security requirement automation framework proposed here may require future updates to align with next-generation AI-driven cybersecurity standards.

Another key limitation is the lack of real-world implementation and validation in military IoBT environments. While the study proposes AI-SysML security frameworks that are theoretically sound, empirical testing through live simulations and operational deployments was not conducted. This limits the ability to assess real-time adaptability, accuracy, and resilience of AI-driven security policies in battlefield conditions (Blasek et al., 2023). Future studies should include field testing of AI-enhanced security automation in military-grade IoBT networks to evaluate performance under adversarial cyberattack scenarios. Lastly, the study does not account for adversarial AI threats, such as poisoning attacks on AI security models or deceptive adversarial inputs (Ahmad et al., 2022). As AI-driven security automation becomes more prevalent, state-sponsored cyber adversaries may attempt to manipulate AI-generated security requirements by injecting misleading data into training models. This remains an unexplored vulnerability, requiring further research into AI adversarial defense mechanisms within the IoBT domain.

Recommendations for Future Research

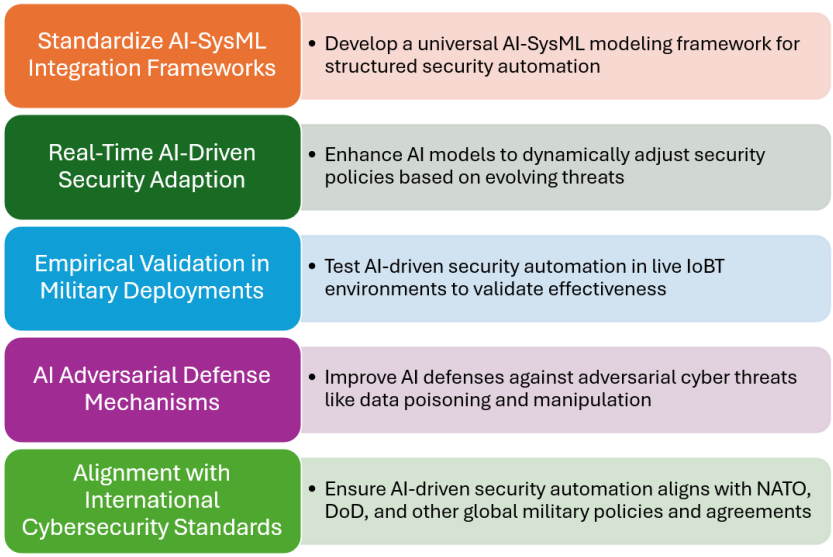
Subsequent research should create standardized AI-SysML integration frameworks to enhance interoperability, traceability, and systematic security modeling in IoBT systems. This study identifies the lack of a universal AI-to-SysML translation mechanism as a significant barrier, hindering the operationalization of AI-generated security needs (Apvrille & Sultan, 2024). Blasek et al. (2023) assert that AI models encounter difficulties operating effectively within engineering workflows without specified input-output links, underscoring the imperative for standardization to guarantee real-time adaptability in IoBT cybersecurity. Furthermore, the progression of AI-driven real-time security adaptation is essential, as existing AI models do not effectively modify security policies in reaction to changing cyber threats (Nomikos et al., 2024). Ahmad et al. (2022) emphasize that static security rules are inadequate against adversarial strategies, hence mandating investigation into deep reinforcement learning (DRL) and AI-driven risk assessment models capable of continuously optimizing security policies according to real-time IoBT battlefield conditions. Furthermore, the empirical validation of AI-augmented security automation via field testing and live simulations should be highlighted.

This study provides a theoretical basis for AI-SysML integration; however, Langleite et al. (2021) underscore the necessity of practical testing in authentic military settings to evaluate resilience against adversarial cyber-attacks in cybersecurity automation. Controlled testing environments evaluate the efficacy of AI-driven security models in detecting and mitigating intrusions, assuring their practical applicability in mission-critical applications. Furthermore, examining AI adversarial defensive mechanisms is crucial to alleviate the threats of data poisoning, model manipulation, and deceptive cyberattacks that can

compromise AI-generated security policies (Shaukat et al., 2020). The rising prevalence of adversarial AI assaults on military cybersecurity systems demands additional investigation into proactive AI-based responses, including adversarial learning and anomaly detection frameworks. Future research should investigate the alignment of AI-driven security automation with international cybersecurity frameworks, such as NATO and DoD standards, to guarantee interoperability and compliance inside multinational military networks (Toth, 2021). AI-driven compliance verification solutions can optimize cybersecurity audits and ensure IoBT systems adhere to increasing military security rules. Subsequent studies can address these research deficiencies, improve the practical implementation of AI-driven security automation, reconcile the disparity between AI and MBSE cybersecurity methodologies, and develop more robust, adaptive cybersecurity frameworks for next-generation IoBT systems (Rosenberg et al., 2024).

Figure 3

Future Research Directions in AI-Driven IoBT Security



Conclusion

This study illustrates that the automation of security requirements driven by AI, combined with Model-Based Systems Engineering (MBSE) and SysML frameworks, improves cybersecurity tactics' efficiency, precision, and flexibility for Internet of Battlefield Things (IoBT) systems. The study tackled significant issues, including manual security requirement derivation ineffectiveness, the lack of defined AI-SysML integration frameworks, and the necessity for real-time adaptability in defense cybersecurity (Apvrille & Sultan, 2024). The results indicate that AI-assisted security engineering diminishes human errors, enhances adherence to military laws, and facilitates real-time security adjustments to emerging cyber threats (Rosenberg et al., 2024). This work utilizes Large Language Models (LLMs) to extract security requirements and SysML for structured representation, thereby connecting automated security intelligence with actual implementation in military Internet of Battlefield Things (IoBT) systems. This research enhances security automation and advances theory by introducing a bidirectional traceability framework, which guarantees that AI-generated security requirements are auditable and consistent with developing cyber rules (Blasek et al., 2023). These findings have direct applications in safeguarding UAV fleets, autonomous battlefield sensors, and military communication networks, ensuring that defense systems remain robust against adversarial cyber threats, including GPS spoofing, jamming, and malware attacks (Nomikos et al., 2024). The ramifications encompass multi-domain military operations, whereby AI-enhanced cybersecurity automation can refine threat detection, response coordination, and compliance validation across terrestrial, aerial, maritime, and extraterrestrial defensive systems (Ahmad et al., 2022).

This study offers a systematic methodology for AI-driven security automation in IoBT systems; nevertheless, additional efforts are required to provide standardized AI-SysML translation frameworks that

guarantee seamless integration across diverse defensive platforms. Future research should investigate real-time AI-driven risk assessment models that can identify and mitigate cyber threats prior to their impact on military operations. Furthermore, conducting live tests of AI-augmented security models in military operations will yield empirical validation, enhancing adaptive security automation tactics for next-generation IoBT systems. This research integrates AI security intelligence with MBSE approaches, facilitating scalable, adaptable, and resilient cybersecurity frameworks that improve military decision-making, maximize operational security, and maintain adherence to developing cybersecurity standards. As AI-driven security automation advances, its significance in military innovation, strategic cybersecurity planning, and multi-domain warfare will become increasingly essential (Apvrille & Sultan, 2024; Rosenberg et al., 2024).

References

Adel, A., & Jan, T. (2024). Watch the skies: a study on drone attack vectors, forensic approaches, and persisting security challenges. *Future internet, 16*(250), 23. Retrieved from https://doi.org/10.3390/fi16070250

Aguilar-Calderon, J.-A., Tripp-Barba, C., Zaldivar-Colado, A., & Aguilar-Calderon, P.-A. (2022, July 2). Requirements engineering for internet of things (lot) software systems development: a systematic mapping study. *Applied sciences, 12*(7582), 1-23. doi:https://doi.org/10.3390/app12157582

Ahmad, K., Abdelrazek, M., Arora, C., Bano, M., & Grundy, J. (2022, December 20). Requirements Engineering for Artificial Intelligence Systems: A Systematic Mapping Study. *Elsevier*, 1–45. doi:https://doi.org/10.48550/arXiv.2212.10693

Alaba, F. A., Othman, M., Hashem, I. A., & Alotaibi, F. (2020, June 15). Internet of Things Security: A Survey. *Journal of Network and Computer Applications, 88*, 10–28. doi:https://doi.org/10.1016/j.jnca.2017.04.002

Apostolopoulos, S. (2022). Internet of military things smart warrior. International Hellenic University, School of Science and Technology. Thessaloniki, Greece: International Hellenic University. Retrieved from https://repository.ihu.edu.gr//xmlui/handle/11544/29945

Apvrille, L., & Sultan, B. (2024). System architects are not alone anymore: automatic system modeling with ai. *12th International Conference on Model-Based Software* (p. 13). Rome, Italy: HAL Open Source. Retrieved from https://telecom-paris.hal.science/hal-04483279/file/apvrille_modelsward2024.pdf

Barbu, F.-M. (2024). Drone warfare - evolution or revolution in military affairs? *Romanian military Thinking(2),* 6–13. Retrieved from https://research.ebsco.com/c/7oqvtd/viewer/pdf/w43fwzf2m5

Blasek, N., Eichenmüller, K., Ernst, B., Götz, N., Nast, B., & Sandkuhl, K. (2023, December 1). Large language models in requirements engineering for digital twins. *Proceedings of the 16th IFIP WG 8.1 Working Conference on the Practice of Enterprise Modeling and the 13th Enterprise Design and Engineering Working Conference*, 15. Retrieved from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiwkNS9-8GGAxXa5MkDHcWoKGsQFnoECBIQAQ&url=https%3A%2F%2Fceur-ws.org%2FVol-3645%2Fdte1.pdf&usg=AOvVaw2DvzmxE61OmNFIN35xL2oD&opi=89978449

Delligatti, L. (2014). *SysML Distilled: A Brief Guide to The Systems Modeling Language.* Upper Saddle River, NJ: Addison-Wesley.

Ersu, C., Petlenkov, E., & Janson, K. (2024). A systematic review of cutting-edge radar technologies: applications for unmanned ground vehicles (UGVs). *Sensors*, 7807. doi:https://doi.org/10.3390/

Feng, Y., Li, M., Zeng, C., & Liu, H. (2020, September 19). Robustness of internet of battlefield things (iobt): a directed network perspective. *Entropy, 22*(1166), 1-15. doi:10.3390/e22101166

Kafakunesu, R., Myburgh, H., & De Freitas, A. (2025, January 10). The internet of battle things: a survey on communication challenges and recent solutions. *Discover Internet of Things, 5(3),* 28. Retrieved from https://doi.org/10.1007/s43926-025-00093-w

Kang, J. J., Yang, W., Dermody, G., Ghasemian, M., Adibi, S., & Haskell-Dowland, P. (2020, November 4). No soldiers left behind: an iot-based low-power military mobile health system design. *IEEE Access, 8*, 201498–201515. doi: 10.1109/ACCESS.2020.3035812

Kitchenham, B., & Charters, S. M. (2007, January). Guidelines for performing systematic literature reviews in software. 66. Retrieved from https://www.researchgate.net/publication/302924724_Guidelines_for_performing_Systematic_Literature_Reviews_in_Software_Engineering

Langleite, R., Griwodz, C., & Johnsen, F. T. (2021). Military applications of internet of things: operational concerns explored in context of a prototype wearable. Oslo, Norway: University of Oslo, Norway. Retrieved from https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/2993/1948731.pdf

Li, K., Wu, Y., Bakar, A., Wang, S., Li, Y., & Wen, D. (2022). Energy system optimization and simulation for low-altitude solar-powered unmanned aerial vehicles. *Aerospace, 9(6)*, 331. doi:https://doi.org/10.3390/aerospace9060331

Ma, M., Liu, K., Luo, X., Zhang, T., & Liu, F. (2020, December). Review of mac protocols for vehicular ad hoc networks. *Sensors (Basel), 20(23),* 6709. doi:https://doi.org/10.3390%2Fs20236709

Marques, N., Silva, R. R., & Bernadino, J. (2024, May 21). Using chatgpt in software requirements engineering: a comprehensive review. *Future internet, 16*(180), 1-21. doi:https://doi.org/10.3390/fi16060180

Martin, J., Westall, J., Kaur, M., Alsuhaim, A., Hridi, A., & Amin, R. (2020). On the efficacy of pub-sub in the emerging internet of battle things. Clemson: clemson university. Retrieved from https://people.computing.clemson.edu/~jmarty/projects/lowLatencyNetworking/ProjectMaterial/EfficacyofpubsubInAdHocWirelessAccessNetworksV3.pdf

McIntyre, J. (2024, December 6). Washington Examiner. Retrieved from www.washingtonexaminer.com: https://www.washingtonexaminer.com/policy/defense/3252080/as-one-of-his-last-acts-defense-secretary-lloyd-austin-signs-off-on-counter-drone-strategy/

More, P., & Phalnikar, R. (2012, April). Generating uml diagrams from natural language specifications. *International journal of applied information systems (IJAIS), 1*(8), 19-23. Retrieved from https://www.academia.edu/download/75441480/Generating_UML_Diagrams_from_Natural_Lan20211130-7215-12dccn3.pdf

Netz, L., Michael, J., & Rumpe, B. (2024). From natural language to web applications: using large language models for model-driven software engineering. *Modellierung 2024*, 179-195. doi:https://doi.org/10.18420/modellierung2024_018

Nomikos, N., Giannoopoulos, A., Kalafatelis, A., Ozduran, V., Trakadas, P., & Karagiannidis, G. K. (2024, January 5). Improving connectivity in 6g maritime communication networks with uav swarms. *Ieee access, 12*, 18739–18751. doi: 10.1109/ACCESS.2024.3360133

Object Mangement Group. (2024). *Omg systems modeling language (omg sysml™) part 1: language specification.* OMG. Retrieved from https://safe.menlosecurity.com/https://www.omg.org/spec/SysML/20230201/

Pal, S., Hitchens, M., Rabehaja, T., & Mukhopadhyay, S. (2020, September). Security requirements for the internet of things: a systematic approach. *Sensors, 20*(20), 5897. doi:https://doi.org/10.3390/s20205897

Perez, A. J., & Zeadally, S. (2021, October 14). Recent advances in wearable sensing technologies. *Sensors, 21*(20), 6828. doi:https://doi.org/10.3390%2Fs21206828

Phadke, A., & Medrano, A. F. (2022, November 3). Towards resilient uav swarms—a breakdown of resiliency requirements in uav swarms. *Drones, 6*(340), 1-39. doi:https://doi.org/10.3390/drones6110340

Phojanamongkolkij, N., VanGundy, B., Polavarapu, R., Levitt, I., & Brown, B. (2023). Requirement discovery using embedded knowledge graph with chatgpt. *AI4SE & SE4AI Research and Application Workshop* (p. 13). Windsor Locks, CT: NASA. Retrieved from https://ntrs.nasa.gov/api/citations/20230013353/downloads/AI4SE_SERC2023_STRIVES.pdf

Ray, P. P. (2023). Chatgpt: a comprehensive review of background, applications, key challenges, bias, ethics, limitations, and future scope. *Internet of things and cyber-physical systems, 3*, 121–154. doi:https://doi.org/10.1016/j.iotcps.2023.04.003

Rosenberg, D., Weilkiens, T., & Moberley, B. (2024). *Ai-assisted mbse with sysml: an integrated systems/software approach.* Las Vegas, NV, USA: MBSE4U.

Saffre, F., Hildmann, H., & Hanny, K. (2021, July 03). The design challenges of drone swarm control. *18th International Conference, EPCE 2021, Held as Part of the 23rd HCI International Conference, HCII 2021, Virtual Event, July 24–29, 2021, Proceedings. 12767*, pp. 408–426. VTT. Retrieved from https://cris.vtt.fi/ws/portalfiles/portal/52430289/2021.Saffre.HCII2021_submitted.pdf

Shaukat, K., Luo, S., Chen, S., & Liu, D. (2020). Cyber threat detection using machine learning techniques: a performance evaluation perspective. *2020 International conference on cyber warfare and security (iccws)*, 1-6. doi:10.1109/ICCWS48432.2020.9292388

Stocchero, J. M., Silva, C. A., Silva, L. d., Lawisch, M. A., dos Anjos, J. C., & de Freitas, E. P. (2023, May). Secure command and control for internet of battle things using novel network paradigms. *Ieee communications magazine, 61*(5), 166-172. doi:10.1109/MCOM.001.2101072

Toth, A. (2021). Internet of things vulnerabilities in military environments. *Vojenské rozhledy*(3), 45-58. doi:10.3849/2336-2995.30.2021.03

U.S. Department of Homeland Security. (2016). Strategic principles for securing the internet of things (iot). Homeland Security. Washington D.C.: Department of Homeland Security. Retrieved from https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf

Werbinska-Wojciechowska, S., Giel, R., & Winiarska, K. (2024). Digital twin approach for operation and maintenance of transportation system—systematic review. *Sensors*, 6069. doi:https://doi.org/10.3390/s24186069

Xi, Z., Chen, W., Guo, X., He, W., Ding, Y., Hong, B., . . . Zhang, Q. (2025, January 17). The rise and potential of large language model based agents: a survey. *Science china information sciences, 68*, 86. doi:https://doi.org/10.1007/s11432-024-4222-0

Zheng, S., Su, Y., Zhuang, J., Tang, Y., & Yi, G. (2024). Fixed-time path-following-based underactuated unmanned surface vehicle dynamic positioning control. *Journal of marine science and engineering, 12*, 551. doi:https://doi.org/10.3390/jmse12040551