Enhancing Battlefield Awareness: Integration of IoMT Sensors and Networks in National Defense Systems

Aris Sarjito*1), Nora Lelyana2)
[1]Republic of Indonesia Defense University, Indonesia
[2]Hang Tuah University, Indonesia

*E-mail: arissarjito@gmail.com[1], nora.lelyana@hangtuah.ac.id[2]

Abstract

The integration of the Internet of Military Things (IoMT) into national defense systems presents both opportunities and challenges for enhancing battlefield awareness and decision-making. This study explores the technical and operational barriers to IoMT deployment, such as interoperability, network bandwidth limitations, energy consumption, and cybersecurity vulnerabilities. Using qualitative research methods based on secondary data from academic articles, defense reports, and technical documents, the study investigates how these challenges impede the effective use of IoMT in military operations. The research findings highlight key issues such as the lack of standardized communication protocols across devices, the need for low-latency networks, and the heightened cybersecurity risks posed by a large number of interconnected devices. Furthermore, the study underscores the importance of energy-efficient solutions to ensure continuous device operation in combat zones. Conclusions suggest that addressing these challenges through standardization, enhanced cybersecurity measures, and adopting emerging technologies such as AI and blockchain is essential for realizing IoMT's potential. Future research should focus on human and organizational factors, geopolitical concerns, and sustainability in IoMT deployment.

Keywords : *cybersecurity, interoperability, IoMT, military operations, network latency*

1. INTRODUCTION

The growing complexity of modern warfare has driven national defense systems to adopt advanced technologies that improve situational awareness, enhance decision-making, and ensure rapid, coordinated responses. Among these innovations, the Internet of Military Things (IoMT) has emerged as a key enabler of battlefield awareness, where sensors, devices, and communication networks are integrated to provide real-time intelligence. The integration of IoMT sensors and networks allows military forces to gather, process, and share data on an unprecedented scale, transforming the traditional battlefield into a dynamic and responsive ecosystem. This reseach explores the state-of-the-art research in IoMT applications, focusing on how these technologies are enhancing battlefield awareness in national defense systems.

IoMT refers to the network of interconnected devices and sensors that collect and exchange information within military environments. These systems offer real-time insights into enemy positions, environmental conditions, and troop movements, thereby enhancing the military's situational awareness. According to Chmielewski et al. (2019), IoMT technologies enable the collection of vast amounts of battlefield data, which is analyzed through artificial intelligence (AI) and machine learning (ML) algorithms to predict enemy actions and assess potential threats. This process, known as sensor fusion, combines data from multiple sources—such as drones, ground-based radars, and wearable devices—into a single, cohesive picture of the battlefield.

The integration of IoMT devices into defense systems has several key advantages. First, it provides real-time surveillance and reconnaissance, allowing commanders to make informed decisions based on live data. As highlighted by (Pasdar et al., 2024), the use of IoMT-connected drones and satellite imagery can offer high-resolution, up-to-the-minute information about enemy movements, significantly improving response times in combat situations. This level of visibility is crucial for making rapid tactical decisions, particularly in environments where conditions can change unpredictably.

The backbone of IoMT-based battlefield awareness is the underlying communication network that links various sensors and devices. Advances in 5G technology and low-power wide-area networks (LPWANs) have made it possible to deploy IoMT sensors across vast distances, connecting them to central command centers in real time. Current research by (Rao et al., 2023) shows that these networks are not only fast and reliable but also capable of maintaining secure communication even in contested environments. The redundancy built into modern networks ensures that data continues to flow even if certain nodes are compromised, which is vital for maintaining operational integrity during combat.

Another critical feature of IoMT-enhanced networks is their ability to support edge computing, where data processing occurs close to the source rather than at a centralized location. By processing data at the edge of the network, IoMT devices reduce latency, enabling faster decision-making on the battlefield. (Awotunde et al., 2021) explain that edge computing helps minimize delays in communication between soldiers and command units, ensuring that critical data is delivered and acted upon in real time. This capability can be particularly beneficial in combat zones, where split-second decisions are essential for mission success.

Despite the benefits, integrating IoMT sensors and networks into defense systems poses several challenges. One of the foremost concerns is cybersecurity. Given the sensitive nature of military operations, IoMT devices are prime targets for cyberattacks, and the consequences of compromised systems can be catastrophic. Recent studies (Pasdar et al., 2024) highlight that while encryption and secure communication protocols have advanced, the sheer number of connected devices creates numerous entry points for potential adversaries. Developing robust cybersecurity measures, including blockchain-based encryption and quantum-resistant algorithms, is essential for ensuring the integrity of IoMT systems.

Another challenge lies in the interoperability of IoMT devices. National defense systems often comprise equipment from various manufacturers, making it difficult to integrate these systems seamlessly. Research by (Priyadarshi & Gheisari, 2024) suggests that adopting open standards for IoMT devices can help address this issue, ensuring that sensors and networks from different providers can communicate and share data effectively. Achieving interoperability is particularly important for multinational defense coalitions, where forces from different nations must collaborate in joint operations.

Looking forward, the role of IoMT in enhancing battlefield awareness is expected to expand as AI and ML algorithms become more sophisticated. Predictive analytics, enabled by these technologies, will allow military forces to anticipate enemy movements and preemptively deploy resources. Furthermore, advances in autonomous systems—such as unmanned aerial vehicles (UAVs) and ground robots—will rely on IoMT networks to navigate and operate autonomously in hostile environments. Research by (Burcham, 2022) highlights the growing potential for integrating IoMT with autonomous defense systems, paving the way for smart warfare where machines assist or even replace humans in certain combat roles.

Moreover, the development of next-generation communication technologies, such as 6G, will further enhance the capabilities of IoMT networks. With higher bandwidth, faster speeds, and lower latency, these networks will support the transmission of even more complex data sets, such as 3D battlefield simulations and augmented reality (AR) interfaces for soldiers on the ground.

The integration of the Internet of Military Things (IoMT) sensors and networks has become a focal point of modern defense strategies due to its potential to improve battlefield awareness and operational efficiency. However, several challenges exist regarding the effective deployment and utilization of these technologies in national defense systems. This essay discusses the statement of the problem, research objectives, and research questions that underpin the study on enhancing battlefield awareness through the integration of IoMT sensors and networks.

The Internet of Medical Things (IoMT) offers great potential for enhancing battlefield awareness through real-time data collection and monitoring. However, its integration into national defense systems faces significant challenges. One key issue is the complexity of creating seamless communication between diverse sensors and devices across different platforms, as continuous data flow is essential but difficult to manage (Rao et al., 2023). Cybersecurity is another major concern, with IoMT networks introducing multiple entry points for potential cyberattacks (Pasdar et al., 2024). Protecting these systems in high-stakes military environments is critical. Additionally, ensuring real-time data transmission with minimal latency requires advanced network infrastructure, posing technical and logistical hurdles (Awotunde et al., 2021). Previous studies have identified advancements in sensor technology, cybersecurity frameworks, and network protocols as potential solutions (Rao et al., 2023; Pasdar et al., 2024; Awotunde et al., 2021). This article builds on these findings, offering novel strategies to improve secure, real-time IoMT integration for battlefield awareness.

Despite the potential benefits of IoMT in enhancing battlefield awareness, there are significant challenges in integrating these technologies into national defense systems. The first problem involves the complexity of creating seamless communication between a diverse range of sensors and devices across various platforms. IoMT networks rely on continuous data flow from multiple sensors, and the integration of such diverse systems can be problematic (Rao et al., 2023). Additionally, cybersecurity is a critical concern, as the vast network of interconnected IoMT devices creates multiple entry points for potential cyberattacks (Pasdar et al., 2024). The ability to secure these systems against adversaries is a growing challenge, especially in high-stakes military environments.

Moreover, ensuring real-time data transmission and reducing latency during critical operations require cutting-edge network infrastructure, which poses technical and logistical hurdles (Awotunde et al., 2021).

Research Objectives

The research objectives of this study are threefold. First, it aims to investigate the current challenges associated with integrating IoMT sensors and networks into national defense systems, providing a comprehensive overview of the technical, logistical, and security-related difficulties encountered during adoption. Second, it seeks to evaluate the effectiveness of IoMT in enhancing battlefield awareness by assessing how real-time data collection and analysis from IoMT networks improve the situational awareness of military commanders through timely and accurate information. Finally, the study aims to develop a framework for optimizing the integration of IoMT sensors and networks, with a focus on enhancing security and interoperability. This objective intends to design a scalable and secure architecture that ensures smooth integration and efficient operation of IoMT devices across various military platforms.

2. RESEARCH METHOD

This research employs a qualitative approach to explore the integration of Internet of Military Things (IoMT) sensors and networks in national defense systems, focusing on battlefield awareness. According to Creswell (2014), qualitative research emphasizes the exploration of complex social or technical issues by analyzing narrative and contextual data. In this study, secondary data, including government defense reports, academic papers, and technical documents, is used to assess the challenges and opportunities of IoMT integration.

The method includes document and content analysis, which systematically reviews and interprets military guidelines, technical specifications, and strategic documents. Thematic analysis is applied to identify recurring themes, such as network security, interoperability, and real-time data transmission. This approach enables a comprehensive understanding of the key factors influencing IoMT adoption.

To ensure validity, triangulation is used by comparing multiple data sources, enhancing the reliability of findings. This research offers insights into how IoMT technologies enhance battlefield awareness while addressing integration challenges.

3. FINDINGS AND DISCUSSION

Research Findings

The integration of IoMT (Internet of Military Things) sensors and networks into national defense systems is a significant advancement in military technology. However, despite the potential benefits of enhanced real-time battlefield awareness and improved decision-making capabilities, several technical and operational challenges impede the full deployment and effectiveness of IoMT systems. These challenges are critical to address for IoMT to become a reliable and integral part of defense operations.

The table below summarizes the main challenges associated with integrating IoMT into national defense systems, including interoperability, network bandwidth and latency issues, energy consumption, and cybersecurity vulnerabilities. The findings highlight the complexity of the problems and the necessity for targeted strategies to overcome them.

Table 1. Research Findings: IoMT Integration Challenges in National Defense Systems

Challenge	Description	Sources
Network Bandwidth and Latency Issues	IoMT networks must handle vast amounts of data in real-time, particularly in combat scenarios. Network congestion and high latency can lead to delayed or incomplete data transmission, affecting decision-making on the battlefield.	(Awotunde et al., 2021; Burcham, 2022)
Energy Consumption and Power Supply	IoMT devices require significant energy, especially when transmitting data over long distances or running advanced algorithms. Energy constraints reduce operational duration and effectiveness, necessitating energy-efficient solutions.	(Burcham, 2022; Chmielewski et al., 2019)
Cybersecurity Vulnerabilities	The large number of IoMT devices creates multiple entry points for potential cyberattacks. Securing IoMT networks requires robust encryption, secure communication channels, and constant monitoring, but real-time requirements create a performance-security trade-off.	(Burcham, 2022; Pasdar et al., 2024)

Source: proceed by author, 2024

After examining these key challenges, it becomes clear that overcoming these barriers requires coordinated efforts across various technological domains. Ensuring seamless interoperability, addressing network limitations, optimizing energy efficiency, and improving cybersecurity are essential for the success of IoMT networks in military operations. These areas represent critical points for future research and development in national defense technology. By tackling these issues, IoMT can significantly enhance military efficiency, situational awareness, and security on the battlefield.

This analysis shows that achieving the full potential of IoMT requires not only technological innovation but also strategic policymaking and collaborative development between military institutions, technology companies, and regulatory bodies.

Interpretation of Research Findings

The research findings reveal several significant challenges in integrating IoMT (Internet of Military Things) sensors and networks into national defense systems. Each of these challenges has profound implications for the successful deployment of IoMT technologies in enhancing real-time battlefield awareness and improving decision-making capabilities.

Interoperability of IoMT Devices

One of the primary obstacles identified is the lack of interoperability between the diverse range of IoMT devices. The findings indicate that different devices, including drones, ground sensors, and wearable technologies, are often developed by different manufacturers and operate using incompatible protocols. This lack of standardization limits the seamless communication required for an integrated operational picture on the battlefield. (Concha Salor & Monzon Baeza, 2023) emphasize the need for common communication protocols, data formats, and sensor interfaces. The current fragmentation complicates not only the initial deployment of IoMT systems but also their scalability in dynamic combat environments. As military systems rely on a cohesive flow of data for accurate situational awareness, the lack of interoperability creates gaps in decision-making, ultimately affecting military efficiency.

Network Bandwidth and Latency Issues

IoMT devices generate a substantial volume of real-time data, which national defense systems must process and transmit efficiently. The findings indicate that network congestion and insufficient bandwidth, especially in high-intensity combat scenarios, can slow data transmission and compromise the timely delivery of critical information to commanders (Blumberg, 2020). High latency further exacerbates the problem, causing delays in data transmission, which can lead to outdated information being used in tactical decisions (Jiang et al., 2018). These issues suggest that the current infrastructure may not be robust enough to support the high demands of IoMT technologies, particularly in environments with limited network coverage. The need for low-latency networks, such as 5G, is clear, but deploying such technologies in combat zones presents additional logistical challenges. Without addressing these network performance issues, IoMT systems will struggle to deliver their full potential for real-time battlefield awareness.

Energy Consumption and Power Supply

Energy consumption is another critical challenge highlighted in the findings. IoMT devices, particularly those deployed in the field, require significant energy to function over extended periods. High energy consumption not only limits the operational duration of these devices but also creates logistical burdens, such as the need for frequent battery replacements or recharges. In combat zones, ensuring a continuous power supply is particularly challenging (Madonna et al., 2018). This issue directly impacts the reliability and effectiveness of IoMT systems, as energy constraints can cause devices to operate at reduced capacity or fail altogether. The findings underscore the need for energy-efficient solutions, such as energy-harvesting technologies and low-power communication protocols. Addressing energy consumption is crucial to ensuring the sustainability and reliability of IoMT in military operations.

Cybersecurity Vulnerabilities

The findings also reveal that cybersecurity is one of the most pressing concerns in IoMT integration. With each IoMT device representing a potential entry point for cyberattacks, the sheer scale of interconnected devices increases the overall vulnerability of the system. (Ahmed et al., 2024) point out that these devices, if compromised, could lead to severe consequences, such as data breaches, communication disruptions, or manipulation of autonomous systems like drones. The challenge lies in securing IoMT systems while maintaining real-time communication and low-latency performance. Encryption protocols and secure communication channels are essential for protecting IoMT networks, but balancing security with performance remains a key challenge. The findings suggest that robust encryption methods, lightweight security solutions for resource-constrained devices, and constant monitoring of IoMT networks are necessary to mitigate cybersecurity risks. Without adequate protection, the vulnerability of IoMT systems could undermine their effectiveness in critical military operations.

Comparison with Literature

The integration of IoMT (Internet of Military Things) into national defense systems has been explored extensively in this research, highlighting critical challenges such as interoperability, network limitations, energy consumption, and cybersecurity vulnerabilities. A comparison of these findings with existing literature reveals both alignment and areas where the literature provides deeper insights or suggests alternative solutions. By comparing the current study with related research, we can better understand how these issues have been addressed previously and identify areas where further advancements are needed.

The table below provides a structured comparison between the key challenges identified in this research and insights from existing literature. It helps to contextualize the challenges and demonstrate how they align or differ from broader discussions in the field.

Table 2. Comparison of IoMT Integration Challenges with Existing Literature

Challenge	Current Study Findings	Comparison with Literature	References
Interoperability of IoMT Devices	Lack of standardized communication protocols complicates integration of IoMT devices from different manufacturers, affecting battlefield awareness.	Kamaldeep et al. (2022) emphasize global military collaboration for unified protocols, aligning with findings on the need for device-level standardization.	(Chmielewski et al., 2019; Kamaldeep et al., 2022)
Network Bandwidth and Latency Issues	Network congestion and high latency affect real-time data transmission, especially in high-stress combat scenarios. Need for low-latency networks like 5G.	Tortonesi et al. (2016) highlight political and logistical challenges in deploying 5G, complementing (Munir et al., 2022) on technical limitations.	(Munir et al., 2022; Tortonesi et al., 2016)
Energy Consumption and Power Supply	High energy consumption limits operational duration of IoMT devices. Energy-efficient solutions are needed, especially in remote areas.	Katalin (2018) suggest military-specific energy solutions like ruggedized batteries, expanding on Chmielewski et al. (2019) regarding energy constraints.	(Chmielewski et al., 2019; Katalin, 2018)

Source: proceed by author, 2024.

After examining the table, it is clear that while there is significant alignment between the current study and existing literature, certain areas, such as the use of blockchain for cybersecurity or AI-driven predictive analytics for decision-making, offer additional pathways for addressing IoMT challenges in military operations. These comparisons suggest that future research should focus on adopting more advanced technologies like AI and blockchain, as well as addressing policy and logistical issues related to infrastructure deployment, to fully harness the potential of IoMT in defense systems.

The integration of these insights can lead to more robust solutions for overcoming the technical and operational barriers that currently limit the effectiveness of IoMT systems.

Theoretical Implications

The integration of the Internet of Military Things (IoMT) into national defense systems presents several important theoretical implications for both military technology and broader fields like systems engineering and cybersecurity. By examining the challenges identified in this research—interoperability, network limitations, energy consumption, and cybersecurity vulnerabilities—these theoretical implications help shape future research directions and development strategies in the defense industry.

Interoperability and Systems Integration Theory

The findings of this study contribute to systems integration theory, particularly in terms of how complex technological systems, like IoMT, interact in real-world scenarios. The lack of standardized communication protocols and the difficulty of achieving seamless interoperability between devices from different manufacturers, as noted by Chituc (2017), reflect broader issues within systems engineering. This research underscores the need for developing universal standards and frameworks that ensure compatibility across a diverse range of devices. Theoretical models related to systems architecture and integration could evolve by incorporating real-time, high-stakes environments like the battlefield into existing frameworks.

(Kamaldeep et al., 2022) also highlight the need for cooperative military frameworks that transcend national boundaries, suggesting that future theoretical work should explore how international standardization and collaboration can be integrated into systems theory to enhance interoperability across multinational defense operations.

Network Latency and Communication Theories

The network bandwidth and latency issues observed in the study have significant implications for communication theories, especially those dealing with real-time data transmission in complex systems. As (Mohammed et al., 2024) note, the delay in data transmission due to network congestion can impact decision-making, which poses a challenge to existing models of real-time communication in high-stakes environments. This raises theoretical questions about how communication latency can be minimized and accounted for in models that depend on real-time information flow, such as network theory and information processing.

(Petrov, 2020) discuss how the deployment of advanced communication technologies, like 5G, requires new theoretical frameworks that address the socio-political complexities of infrastructure implementation, especially in contested or remote areas. Thus, this research suggests that future theoretical work must bridge the gap between communication technology and its logistical challenges in military applications.

Energy Consumption and Sustainability Theories

The challenge of energy consumption in IoMT devices aligns with broader sustainability theories, particularly in the context of technological sustainability in constrained environments. (Dinc et al., 2019) highlight how energy limitations restrict the operational capabilities of IoMT devices, which calls for a rethinking of how energy efficiency is modeled in military technology. (Fraga-Lamas et al., 2016) propose that military-specific energy solutions, such as energy-harvesting technologies, must be incorporated into sustainability theories that deal with high-performance devices in challenging environments.

The implications for sustainability theories are clear: future research must integrate concepts like energy efficiency and renewable energy sources into theoretical frameworks that guide the design and deployment of IoMT systems. This could also influence broader discussions on sustainability in technology-intensive industries beyond the military.

Cybersecurity and Risk Management Theories

The significant cybersecurity vulnerabilities revealed in the study have critical implications for cybersecurity theories, particularly in the area of risk management. (Ghubaish et al., 2020) point out that the vast number of interconnected devices increases the potential for cyberattacks, requiring more robust models of security that account for the unique vulnerabilities of IoMT systems. This suggests that existing risk management theories must be adapted to accommodate the complex, multi-device environments that characterize IoMT networks.

Elsayeh et al. (2021) propose that blockchain technology could be incorporated into cybersecurity frameworks as a method of securing IoMT transactions and data exchanges. This shifts the theoretical discussion toward decentralized security models, where blockchain plays a critical role in ensuring the integrity of IoMT networks. As military operations increasingly rely on IoMT, the theoretical groundwork for understanding cybersecurity in these contexts will need to evolve to include not only encryption and security protocols but also decentralized technologies like blockchain.

Decision-Making Theories and Predictive Analytics

The findings related to real-time data collection and predictive analytics contribute to decision-making theories, especially in the context of military strategy. By incorporating machine learning and AI algorithms, IoMT systems allow commanders to anticipate battlefield developments and make proactive decisions (Pasdar et al., 2024). This calls for the integration of AI-driven predictive analytics into existing decision-making theories, which have traditionally focused on human intuition and real-time data processing.

The theoretical implication here is that decision-making models must evolve to account for AI's role in interpreting vast amounts of data. The shift toward predictive analytics in military decision-making suggests that future theoretical frameworks will need to incorporate both human and machine-based decision-making processes to effectively guide strategic operations in complex environments like the battlefield.

Practical Implications

The research on the integration of IoMT (Internet of Military Things) into national defense systems has several practical implications that can significantly enhance the efficiency, security, and overall operational capabilities of military forces. Addressing the challenges identified in this study—interoperability, network bandwidth, energy consumption, and cybersecurity—has the potential to transform how military operations are conducted in real-time environments. The following are key practical implications based on the research findings.

Improving Interoperability through Standardization

One of the most immediate practical implications is the need for establishing standardized communication protocols and data formats to ensure the interoperability of IoMT devices. The lack of standardization across devices from different manufacturers creates barriers to seamless communication, which can result in delays or incomplete data transfer during critical operations (Raptis et al., 2019). Military organizations, defense contractors, and allied nations must collaborate to create unified standards that allow IoMT devices to communicate and exchange data without compatibility issues.

(Suri et al., 2016) suggest that adopting open standards in military technologies can help create a more integrated and responsive battlefield network. This could be implemented by forming international defense alliances focused on establishing common IoMT protocols, particularly in joint operations. Such standardization would not only enhance the coordination of military operations but also simplify the integration of new devices into existing defense systems.

Enhancing Network Infrastructure for Real-Time Data Transmission

The research highlights the critical need for robust network infrastructures capable of handling the high data volume generated by IoMT devices in real-time combat situations (Dwivedi et al., 2022). Practical measures to address this challenge include investing in low-latency communication technologies, such as 5G and edge computing, to ensure fast and reliable data transmission, even in remote or hostile environments.

(Bajracharya et al., 2023) argue that deploying dedicated military communication networks with enhanced bandwidth and minimal latency could drastically improve real-time decision-making capabilities. Military forces could implement these networks in training exercises and during actual operations, enabling quicker, data-driven decisions that enhance tactical and strategic outcomes. Additionally, integrating edge computing within IoMT systems would allow data to be processed closer to the source, reducing the reliance on centralized data centers and mitigating latency issues.

Adopting Energy-Efficient IoMT Devices

Energy consumption remains a significant barrier to the continuous operation of IoMT devices in the field. (Ahmed et al., 2024) highlight how energy constraints can limit the operational duration of IoMT devices, necessitating frequent recharges or battery replacements. Practical solutions to this challenge involve the development of energy-efficient IoMT devices and the adoption of energy-harvesting technologies that can draw power from environmental sources, such as solar energy or kinetic movement.

(Kang et al., 2020) suggest that ruggedized, long-lasting batteries specifically designed for military use could extend the operational time of IoMT devices in challenging conditions. Furthermore, military organizations could implement low-power communication protocols, enabling devices to conserve energy when high-bandwidth data transmission is not required. These innovations would help ensure that IoMT devices remain operational for extended periods without the need for frequent maintenance, particularly in remote or combat-heavy environments.

Strengthening Cybersecurity Measures

Cybersecurity is another critical practical implication of IoMT deployment. (Thomasian & Adashi, 2021) emphasize that the large number of interconnected devices in IoMT systems increases the risk of cyberattacks, which could disrupt communications, lead to data breaches, or even compromise autonomous military systems. Implementing stronger cybersecurity measures is essential to ensuring the security of IoMT systems in national defense.

One practical approach is to incorporate end-to-end encryption (E2EE) across all IoMT communication channels, ensuring that data remains secure from the point of origin to the final recipient, even if certain parts of the network are compromised (Sharma et al., 2021). Additionally, employing blockchain technology to authenticate and secure IoMT transactions, as suggested by (Pasdar et al., 2024), could prevent unauthorized access to military networks. Military organizations should prioritize the implementation of lightweight encryption algorithms, tailored for low-power IoMT devices, to balance security and operational efficiency. Moreover, regular updates and patches to IoMT software and hardware would help defend against evolving cyber threats, ensuring that military systems remain secure in the long term.

Integrating Predictive Analytics for Enhanced Decision-Making

The ability of IoMT systems to provide real-time data on troop movements, enemy positions, and environmental conditions presents a practical opportunity to enhance military decision-making capabilities. Predictive analytics, powered by AI and machine learning, can analyze this real-time data to forecast potential enemy actions or battlefield outcomes, enabling military commanders to make more informed decisions during combat (Davis, 2019).

Integrating predictive analytics into IoMT systems would enable military forces to stay ahead of adversaries by anticipating threats and proactively deploying resources. Military organizations could implement AI-driven analytics in command centers, where real-time data streams from IoMT devices could be processed to generate actionable intelligence. This would improve both tactical decisions on the battlefield and strategic planning in broader military operations.

Limitations and Future Research

While this study provides valuable insights into the integration of IoMT (Internet of Military Things) in national defense systems, several limitations must be acknowledged. These limitations offer directions for future research that can enhance our understanding and lead to more effective implementations of IoMT technologies in military operations.

Limitations

The research primarily focused on common IoMT devices like drones, ground-based sensors, and wearables, but it did not fully explore the broader range of devices used in military operations, such as autonomous vehicles and satellite systems. This limited scope may affect the comprehensiveness of the findings, as it overlooks the unique challenges and solutions needed for integrating more complex IoMT systems. Additionally, while the study addresses key technical barriers like network latency, interoperability, energy consumption, and cybersecurity, it does not sufficiently explore organizational and human factors that influence IoMT integration, such as training and the adaptability of military command structures.

Furthermore, the research did not deeply consider geopolitical and regulatory challenges that may impact IoMT deployment in multinational defense operations. Differences in national cybersecurity policies and regulatory standards could pose obstacles to IoMT integration during joint operations. The study also focused on established IoMT technologies, without extensive exploration of emerging technologies like quantum computing and 6G networks, which could significantly enhance IoMT capabilities in the future. This reliance on present-day technologies limits the study's ability to anticipate future advancements that may transform IoMT integration.

Future Research Directions

Future research should explore a broader range of IoMT devices, including autonomous underwater vehicles, satellite systems, and advanced robotics used across land, air, sea, and space. Investigating the specific challenges these devices face would offer a more complete understanding of IoMT integration in specialized military operations. Additionally, the human and organizational aspects of IoMT adoption need further study, focusing on how military personnel adapt to these technologies, training requirements, and potential changes to command structures to facilitate IoMT-driven decision-making.

Geopolitical factors are also crucial, as differing national cybersecurity policies and international collaborations may complicate IoMT integration in multinational operations. Examining how organizations like NATO address these challenges would provide valuable insights. Furthermore, future research should explore emerging technologies like quantum computing and 6G, which could enhance IoMT security and data transmission. Sustainability is another key area, with a need to investigate energy-efficient IoMT devices and renewable energy solutions for military applications. Lastly, longitudinal studies tracking IoMT integration over time would provide critical insights into the evolving impact and ongoing challenges in real-world military settings.

4. CONCLUSION

The integration of IoMT sensors and networks into national defense systems presents several technical and operational challenges, including device interoperability, network bandwidth, latency, energy consumption, and cybersecurity risks. The diversity of IoMT devices complicates communication, requiring standardization for seamless operation. Additionally, network limitations in bandwidth and latency hinder real-time data transmission, while energy constraints limit IoMT device effectiveness. Cybersecurity also remains a key concern, with expanded IoMT networks increasing the risk of cyberattacks on defense infrastructure. Addressing these issues will need collaboration between military organizations, technology developers, and policymakers.

Despite these challenges, IoMT significantly enhances battlefield awareness and decision-making by providing real-time data on troop movements, enemy positions, and environmental conditions. This enables commanders to make quicker, more informed decisions, while improving coordination between command centers and field units. However, to fully realize IoMT's potential, issues like network reliability and data management must be addressed to ensure its efficiency in modern military operations.

To mitigate cybersecurity risks and improve interoperability, military organizations must adopt robust encryption methods, lightweight security protocols, and open communication standards.

Zero-trust architectures and emerging technologies like blockchain and quantum-resistant encryption will further enhance the security and interoperability of IoMT systems, ensuring their long-term resilience in national defense operations.

REFERENCES

Ahmed, S. F., Alam, M. S. Bin, Afrin, S., Rafa, S. J., Rafa, N., & Gandomi, A. H. (2024). Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions. *Information Fusion*, *102*, 102060.

Awotunde, J. B., Jimoh, R. G., Matiluko, O. E., Gbadamosi, B., & Ajamu, G. J. (2021). Artificial intelligence and an edge-IoMT-based system for combating COVID-19 pandemic. In *Intelligent Interactive Multimedia Systems for e-Healthcare Applications* (pp. 191–214). Springer.

Bajracharya, R., Shrestha, R., Hassan, S. A., Jung, H., & Shin, H. (2023). 5g and beyond private military communication: Trend, requirements, challenges and enablers. *IEEE Access*.

Blumberg, M. M. S. (2020). The Integrated Tactical Network. *MILITARY REVIEW*.

Burcham, P. M. (2022). *A Comprehensive Literature Review of Autonomous Surveillance Technologies Relating to Dismounted Soldiers*.

Chituc, C.-M. (2017). XML interoperability standards for seamless communication: An analysis of industry-neutral and domain-specific initiatives. *Computers in Industry*, *92*, 118–136.

Chmielewski, M., Kukiełka, M., Gutowski, T., & Pieczonka, P. (2019). Handheld combat support tools utilising IoT technologies and data fusion algorithms as reconnaissance and surveillance platforms. *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, 219–224.

Concha Salor, L., & Monzon Baeza, V. (2023). Harnessing the Potential of Emerging Technologies to Break down Barriers in Tactical Communications. *Telecom*, *4*(4), 709–731.

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. SAGE Publications.

Davis, Z. (2019). Artificial intelligence on the battlefield. *Prism*, *8*(2), 114–131.

Dinc, E., Kuscu, M., Bilgin, B. A., & Akan, O. B. (2019). Internet of everything: A unifying framework beyond internet of things. In *Harnessing the Internet of Everything (IoE) for Accelerated Innovation Opportunities* (pp. 1–30). IGI Global.

Dwivedi, R., Mehrotra, D., & Chandra, S. (2022). Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review. *Journal of Oral Biology and Craniofacial Research*, *12*(2), 302–318.

Elsayeh, M., Ezzat, K. A., El-Nashar, H., & Omran, L. N. (2021). Cybersecurity architecture for the internet of medical things and connected devices using blockchain. *Biomedical Engineering: Applications, Basis and Communications*, *33*(02), 2150013.

Fraga-Lamas, P., Fernández-Caramés, T. M., Suárez-Albela, M., Castedo, L., & González-López, M. (2016). A review on internet of things for defense and public safety. *Sensors*, *16*(10), 1644.

Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-Ali, A., & Jain, R. (2020). Recent advances in the internet-of-medical-things (IoMT) systems security. *IEEE Internet of Things Journal*, *8*(11), 8707–8718.

Jiang, X., Shokri-Ghadikolaei, H., Fodor, G., Modiano, E., Pang, Z., Zorzi, M., & Fischione, C. (2018). Low-latency networking: Where latency lurks and how to tame it. *Proceedings of the IEEE*, *107*(2), 280–306.

Kamaldeep, Malik, M., & Dutta, M. (2022). Security Challenges in Internet of Things (IoT) integrated power and energy (PaE) systems. *Intelligent Data Analytics for Power and Energy Systems*, 555–566.

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

Katalin, B. E. (2018). Possibilities and security challenges of using IoT for military purposes. *Hadmérnök*, *13*(3), 378–390.

Madonna, V., Giangrande, P., & Galea, M. (2018). Electrical power generation in aircraft: Review, challenges, and opportunities. *IEEE Transactions on Transportation Electrification*, *4*(3), 646–659.

Mohammed, S. M., Al-Barrak, A., & Mahmood, N. T. (2024). Enabling Technologies for Ultra-Low Latency and High-Reliability Communication in 6G Networks. *Ingénierie Des Systèmes d'Information*, *29*(3).

Munir, A., Aved, A., & Blasch, E. (2022). Situational awareness: techniques, challenges, and prospects. *AI*, *3*(1), 55–77.

Pasdar, A., Koroniotis, N., Keshk, M., Moustafa, N., & Tari, Z. (2024). Cybersecurity Solutions and Techniques for Internet of Things Integration in Combat Systems. *IEEE Transactions on Sustainable Computing*.

Petrov, A. (2020). *5G, China and the Global Governance of Cyberspace*.

Priyadarshi, R., & Gheisari, M. (2024). *Security and Privacy in Machine Learning for IoHT and IoMT: A Review*.

Rao, S. S., Reddy, E. M., & Tyagi, S. B. (2023). *Next Generation IoMT enabled Smart HealthCare using Machine Learning Techniques*.

Raptis, T. P., Passarella, A., & Conti, M. (2019). Data management in industry 4.0: State of the art and open challenges. *IEEE Access*, *7*, 97052–97093.

Sharma, D., Nawab, A. Z. Bin, & Alam, M. (2021). Integrating M-health with IoMT to counter COVID-19. *Computational Intelligence Methods in COVID-19: Surveillance, Prevention, Prediction and Diagnosis*, 373–396.

Suri, N., Tortonesi, M., Michaelis, J., Budulas, P., Benincasa, G., Russell, S., Stefanelli, C., & Winkler, R. (2016). Analyzing the applicability of internet of things to the battlefield environment. *2016 International Conference on Military Communications and Information Systems (ICMCIS)*, 1–8.

Thomasian, N. M., & Adashi, E. Y. (2021). Cybersecurity in the internet of medical things. *Health Policy and Technology*, *10*(3), 100549.

Tortonesi, M., Morelli, A., Govoni, M., Michaelis, J., Suri, N., Stefanelli, C., & Russell, S. (2016). Leveraging Internet of Things within the military network environment—Challenges and solutions. *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, 111–116.