WWJMRD 2026; 12(01): 09-13
www.wwjmrd.com
International Journal
Peer Reviewed Journal
Refereed Journal
Indexed Journal
Impact Factor SJIF 2017: 5.182 2018: 5.51, (ISI) 2020-2021: 1.361
E-ISSN: 2454-6615

Dr Anjan K Sinha
UPES, Dehradun,
Uttarakhand, India.

Correspondence:
UPES, Dehradun,
Uttarakhand, India.

Internet of Battlefield Things (IoBT): A Systematic Review

Dr Anjan K Sinha

Abstract
Internet of Things (IoT) is the latest trend that in- corporates many technologies in it. People are gradually entering into the IoT era where communication takes place between hu- mans and objects and between objects themselves. The IoT brings a new aspect in Information and Communication Technology (ICT) that associate everyone from every location at any time. It integrates the real world with the data world. The advent of ICT and Radio Frequency Identification (RFID) enables the IoT to become very popular with humans. newlineIt is a rapidly developing framework, where conventional networked objects are connected with the physical entities including home appliances, vehicles, battlefield things, industrial things, etc. Smart entities (also called quotthingsquot) can sense other objects which are close to them and also exchange information with one another with the help of the internet. The significant elements of the IoT is the wireless sensor that accumulate information from the circumstances and controls the same if it needs any modification. Most of the applications offers novel innovative services or im- proves the effectiveness of the existent one. Such applications are disaster management, smart health, environmental monitoring, industrial, agriculture, battlefield surveillance, etc. Among these, the Internet of Battlefield Things (IoBT) application is getting more attention due to its open and unattended environment. Newline Due to the significant characteristics, the IoT is suitable for group-based communication like battlefield networks. It plays an essential role in the battlefield to interconnect various IoBT nodes to communicate with each other. Many battlefield things like combat equipment, war-fighters, vehicles, smart-watches, and smart-spectacles are attached with sensors to accumulate the data from the battlefield network and transfer this information to the responsible person/object to make a real-time decision on military applications. This information should be reliable and secured for a successful mission.

Keywords: component, formatting, style, styling, insert.

I. Introduction

The concept of the" Internet of Battlefield Things" (IoBT) has emerged as a revolutionary approach to modern warfare and military operations, drawing upon the broader technolog- ical framework of the Internet of Things (IoT). [1] IoT repre- sents a network of interconnected devices that communicate, share data, and operate in real-time environments. [2] The IoBT takes this concept a step further by focusing on military applications where the battlefield environment is augmented by a variety of smart devices, sensors, vehicles, weapons systems, and communication tools that work cohesively to enhance situ- ational awareness, decision-making, and combat effectiveness. As warfare continues to evolve in the age of digitization and autonomous systems, the IoBT is a central element shaping future military strategies. This paper delves into the critical aspects of IoBT, examining its architecture, key components,

Identify applicable funding agency here. If none, delete this. technological innovations, and potential challenges, as well as their implications for national security and military operations in the 21st century.

II. Defining the Internet of Battlefield Things (IoBT)

The Internet of Battlefield Things refers to an ecosystem of interconnected devices and systems designed to operate in combat zones. [3] These systems can include sensors, drones,

autonomous vehicles, wearable devices, and intelli- gent command-and-control systems, all capable of collecting, analysing, and acting on data in real time. The goal of IoBT is to improve a military unit's ability to perceive its surroundings, respond more quickly to changing conditions, and increase combat effectiveness by enhancing command and control systems. The defining features of IoBT are connectiv- ity, intelligence, and interoperability. Connectivity ensures that all battlefield elements, from soldiers to machines, are linked and able to communicate with one another. [4] Intelligence refers to the use of artificial intelligence (AI) and machine learning (ML) algorithms to process data, make decisions, and even automate certain aspects of warfare. Interoperability focuses on ensuring that different systems, whether developed by different nations or manufacturers, can work together in an integrated fashion. [5] IoBT integrates various technologies, including IoT, AI, cloud computing, big data, and autonomous systems, to form a cohesive network. As a result, IoBT enables real-time situational awareness, dynamic command and control, and the ability to quickly adapt to evolving battlefield conditions.

A. Key Components of IoBT

[6] The IoBT ecosystem consists of several key components that work together to create a comprehensive and efficient battlefield network. These components include:

1) Sensors and Devices: Sensors play a crucial role in IoBT, as they gather data from the battlefield and relay it to central command systems for analysis. Sensors can be placed on soldiers, vehicles, or unmanned systems, such as drones. These devices can detect a wide range of information, including temperature, movement, sound, chemical signatures, and enemy positions. [7] Wearable devices on soldiers can monitor vital signs, while environmental sensors can detect potential threats, such as toxic gases or enemy movements.
2) Unmanned Aerial Vehicles (UAVs) and Drones: Drones are integral to IoBT due to their versatility in surveillance, reconnaissance, and attack operations. Equipped with cam- eras, radar, and other sensor arrays, drones can provide real- time intelligence to ground forces and command centers. Furthermore, autonomous drones with AI-driven navigation systems can patrol, identify targets, and engage in offensive or defensive actions with minimal human intervention.
3) xAutonomous Ground Vehicles (AGVs): Autonomous ground vehicles are used to transport supplies, evacuate wounded soldiers, or engage in combat missions. AGVs are equipped with advanced AI systems that enable them to navigate the battlefield independently, avoiding obstacles, identifying threats, and responding to commands from human operators or higher-level AI systems.
4) Robotic Systems and Swarm Technologies: Robotic systems are becoming a common feature in IoBT, with ap- plications ranging from bomb disposal to direct combat roles. The introduction of swarm technology, where groups of robots or drones collaborate and operate as a cohesive unit, further enhances the battlefield's versatility. Swarm intelligence al- lows autonomous systems to perform complex tasks, such as coordinating an attack on an enemy position or establishing a defensive perimeter.
5) Artificial Intelligence and Machine Learning: AI and ML are the driving forces behind the autonomous capabilities of IoBT systems. AI algorithms can process vast amounts of data collected from sensors and devices, identifying patterns and providing commanders with actionable intelligence. ML allows these systems to learn from experience, improving their accuracy and effectiveness over time. AI systems can also automate decision-making processes, determining the best course of action based on current battlefield conditions.
6) Cloud Computing and Edge Computing: Cloud com- puting and edge computing are essential components of IoBT, providing the necessary infrastructure for data storage, pro- cessing, and communication. Cloud computing enables large- scale data analysis by central command systems, while edge computing brings computational power closer to the battle- field, reducing latency and ensuring real-time decision- making. Edge devices, such as drones or ground vehicles, can process data locally, ensuring that critical decisions can be made on the battlefield without relying on a remote command center.
7) Cybersecurity and Encryption Technologies: The inter- connected nature of IoBT makes it vulnerable to cyberattacks and data breaches. Cybersecurity technologies are crucial to safeguarding IoBT networks and ensuring that data integrity and confidentiality are maintained. Encryption technologies, secure communication protocols, and AI- based cybersecurity systems work together to protect the network from hacking, signal jamming, and other cyber threats.
8) Command and Control Systems: IoBT enhances tradi- tional command and control systems by enabling commanders to access real-time data from the battlefield. These systems integrate information from multiple sources, providing com- manders with a comprehensive view of the battlefield. AI and ML algorithms help commanders make data-driven decisions, such as determining troop movements, prioritizing targets, and allocating resources.

III. IoBT Applications in Modern Warfare

The IoBT concept has numerous applications in modern warfare, particularly in areas such as situational awareness, decision-making, logistics, and combat effectiveness. [8] The description of application is presented in subsections below as well as graphical representations is shown in Figure 2.

A. Enhanced Situational Awareness

One of the most significant advantages of IoBT is its ability to provide real-time situational awareness. Sensors, drones, and wearable devices collect data from the battlefield, which is then analyzed by AI systems to provide commanders with a comprehensive understanding of the operational environment. This data includes enemy positions, troop movements, and environmental conditions, all of which can be used to make informed decisions. For example, UAVs equipped with infrared cameras can detect enemy forces at night or in low-visibility conditions.

Meanwhile, ground-based sensors can monitor troop movements, providing commanders with early warning of potential attacks. The data from these sensors is transmitted to command centers in real-time, allowing for quick decision-making and rapid responses.

B. Autonomous Combat Systems

Autonomous combat systems, including UAVs, AGVs, and robotic systems, are transforming the way militaries con- duct operations. These systems can perform tasks such as reconnaissance, target identification, and even direct combat roles without the need for human intervention. For instance, autonomous drones can conduct airstrikes, while AGVs can patrol borders or engage enemy forces on the ground. The use of AI in these systems allows them to make decisions in real-time, responding to battlefield conditions and adapting to changing situations. For example, a swarm of drones could be deployed to overwhelm enemy defenses or conduct coordinated attacks on multiple targets simultaneously.

C. Improved Command and Control

IoBT significantly enhances command and control capa- bilities by providing commanders with access to real-time data from the battlefield. Commanders can use this data to monitor troop movements, assess the effectiveness of ongoing operations, and make adjustments to tactics as needed. IoBT also allows for more efficient communication between units, ensuring that all forces are working towards the same objec- tive. AI systems can assist commanders in making decisions by analysing data and providing recommendations. For instance, AI algorithms could analyse the movements of enemy forces and predict their next actions, allowing commanders to posi- tion their troops accordingly.

D)Logistics and Supply Chain Optimization

The IoBT can also be used to optimize logistics and supply chain management in military operations. Autonomous vehicles can be used to transport supplies, ensuring that troops have the resources they need in the field. IoT sensors can monitor the condition of supplies, such as ammunition or medical equipment, and notify commanders when resources are running low. Additionally, AI systems can optimize sup- ply routes, ensuring that supplies are delivered quickly and efficiently. For example, AI algorithms could analyse weather conditions, enemy activity, and terrain to determine the best route for delivering supplies to a remote outpost.

E) Medical Support and Casualty Evacuation

IoBT can play a critical role in providing medical support on the battlefield. Wearable devices can monitor soldiers' vital signs and transmit data to medical teams in real-time. [9] This allows medics to assess a soldier's condition remotely and provide immediate treatment if necessary. In cases where evacuation is required, autonomous vehicles can transport wounded soldiers to medical facilities without putting human lives at risk. IoT-enabled medical devices, such as drones equipped with first-aid kits, can also deliver critical supplies to injured soldiers in the field. AI systems can assist medics in diagnosing injuries and recommending treatment options based on the data collected from wearable devices.

F) Electronic Warfare and Cyber Defence

IoBT introduces new capabilities in the realm of electronic warfare and cyber defence. AI-driven systems can detect and respond to cyber threats in real-time, ensuring that IoBT networks remain secure. For instance, AI algorithms can identify unusual network activity, such as a potential hacking attempt, and take immediate action to neutralize the threat. Additionally, IoBT systems can be used in offensive electronic warfare operations. Autonomous drones equipped with elec- tronic jamming devices can disrupt enemy communications or disable radar systems, giving friendly forces a tactical advantage.

IV. Challenges and Risks

While the IoBT offers numerous benefits, it also presents several challenges and risks that must be addressed to ensure its effectiveness. [10]

A. Cybersecurity Vulnerabilities

The interconnected nature of IoBT makes it a prime target for cyberattacks. [11] Hackers could infiltrate IoBT networks and compromise sensitive data, disrupt communications, or even take control of autonomous systems. To mitigate this risk, robust cybersecurity measures must be implemented, including encryption, secure communication protocols, and AI-based threat detection systems.

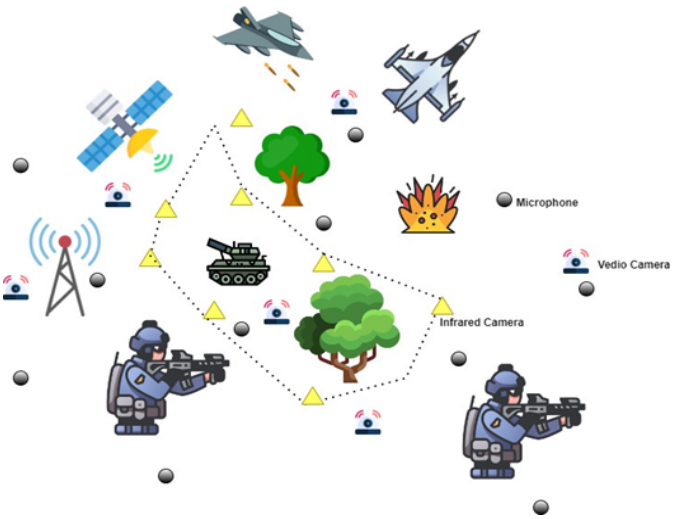

Fig. 1: Key of Components of Battlefield.

B) Data Overload

The vast amount of data generated by IoBT systems can overwhelm commanders and decision-makers. Analyzing and interpreting this data in real-time is a significant challenge, especially in the heat of battle. AI systems can help by filtering and prioritizing data, but there is still the risk of information overload, which could lead to delayed or incorrect decisions.

C) Autonomy and Ethical Concerns.

The increasing use of autonomous systems in warfare raises ethical concerns. Autonomous drones and robots have the potential to make life-and-death decisions without human intervention. [12] This raises questions about accountability and the potential for unintended consequences, such as civilian casualties or friendly fire incidents.

D) Interoperability and Standardization

The success of IoBT depends on the ability of different systems and devices to work together seamlessly. However, achieving interoperability between devices developed by dif- ferent manufacturers or nations can be challenging. [13] Stan- dardization efforts are needed to ensure that IoBT systems can communicate and operate effectively across different plat- forms.

E) Cost and Infrastructure Requirements
Developing and deploying IoBT systems can be expensive, particularly for smaller nations or military organizations with limited budgets. The infrastructure required to support IoBT, including cloud computing, edge computing, and communi- cation networks, may not be readily available in all regions. Additionally, maintaining and upgrading IoBT systems can be costly and resource-intensive

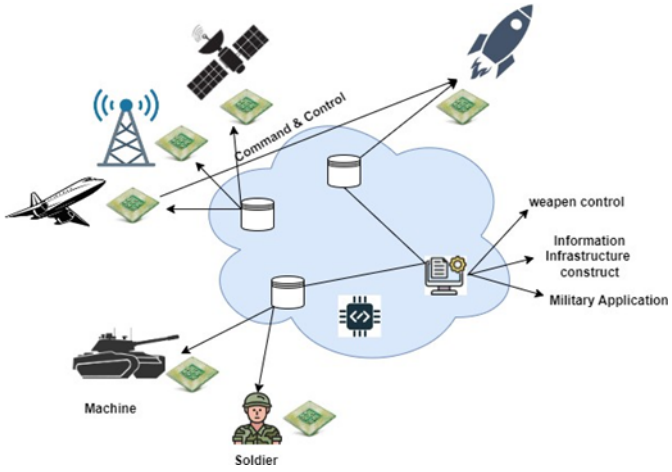

Fig. 2: Applications of Battlefield.

V. Future of IoBT

As military technology continues to advance, the Internet of Battlefield Things is expected to play an increasingly important role in shaping the future of warfare. [14] The integration of AI, autonomous systems, and advanced sensors will enable militaries to conduct operations more efficiently, with greater precision and reduced risk to human life. Looking ahead, several trends are likely to shape the evolution of IoBT:

A. AI-Driven Decision Making
AI systems will play a more prominent role in decision-making processes on the battlefield. As AI algorithms become more sophisticated, they will be able to analyze complex data sets, identify patterns, and provide commanders with actionable intelligence. This will enable militaries to respond more quickly to changing conditions and make more informed tactical decisions.

B. Advanced Swarm Technologies
Swarm technologies, where groups of autonomous drones or robots work together, are expected to become more prevalent in IoBT. Swarm intelligence allows these systems to perform complex tasks, such as coordinated attacks or defensive ma- noeuvres, with minimal human oversight. Future swarms may consist of hundreds or even thousands of autonomous units, operating as a cohesive force.

C. Increased Autonomy
The trend towards increased autonomy in military sys- tems will continue, with more advanced autonomous vehicles, drones, and robots being deployed on the battlefield. These systems will be able to operate independently for extended periods, making decisions based on real-time data and adapting to changing conditions.

D. Enhanced Cyber Defence Capabilities
As cyber threats become more sophisticated, IoBT systems will need to be equipped with advanced cybersecurity measures. [15] AI-driven cybersecurity systems will play a crucial role in detecting and responding to cyberattacks in real time, ensuring the integrity of IoBT networks.

E. Human-Machine Teaming
While autonomous systems will play a more significant role in future warfare, human oversight will remain essential. Human-machine teaming, where humans and AI systems work together to achieve a common goal, will become a central feature of IoBT. Commanders will rely on AI systems to analyse data and provide recommendations, while retaining the final decision-making authority.

F. Indian Scenario
The implementation of theatre commands and the ever-known threat from the neighbouring countries will force the Indian Military to adopt the best practices of IoBT. [16] The all-theatre integration including all services on a common platform will provide battlefield awareness and this is a key to win a War if it so happens. Integration of different platforms of all three services to a common platform and sharing of frequencies will enhance the compatibility and synergy of the Indian Military. The challenges to these remain:

1. Mindset of Leaders to change and accept the homogenisation of forces.:
2. Having a common Preci for all the three services and integration philosophy right from training academies.:
3. Uniformity in mode of Communication among three Services:
4. Concurrent common Practices for support Logistics to include Ration, Reliability Engineering support to Military Eqpts.:
5. Review of Legal codes and Acts of all three services for a common discipline code of conduct.:
6. Farming of rules for conduct for the Department of Military Affairs with other Government Agencies and Inter Service Relations.:

VI. Conclusion

The Internet of Battlefield Things represents a transformative shift in military operations, leveraging the power of interconnected devices, AI, and autonomous systems to enhance combat effectiveness and improve decision-making. While IoBT offers numerous advantages, it also presents significant challenges, including cybersecurity risks, data overload, and ethical concerns. As technology continues to evolve, militaries must address these challenges to fully realize the potential of IoBT and ensure that it is used responsibly and effectively in future conflicts. The future of warfare will be shaped by the integration of IoBT systems, and militaries that embrace this technology will be better positioned to succeed in an increasingly complex and dynamic battlefield environment.

References

1. S. Russell and T. Abdelzaher, “The internet of battlefield things: the next generation of command, control, communications and intelligence (c3i) decision-making,” in MILCOM 2018-2018 IEEE Military Commu- nications Conference (MILCOM), pp. 737–742, IEEE, 2018.
2. M. Wigness, T. Pham, S. Russell, and T. Abdelzaher, “Efficient and resilient edge intelligence for the internet of battlefield things,” NATO S&T Journal, 2021.
3. J. Lee, K. Marcus, T. Abdelzaher, M. T. A. Amin, A. Bar-Noy, W. Dron, R. Govindan, R. Hobbs, S. Hu, J.-E. Kim, et al., “Athena: Towards decision-centric

anticipatory sensor information delivery," Journal of Sensor and Actuator Networks, vol. 7, no. 1, p. 5, 2018.
4. G. Rovatsos, V. V. Veeravalli, D. Towsley, and A. Swami, "Quickest detection of anomalies of varying location and size in sensor networks," IEEE Transactions on Aerospace and Electronic Systems, vol. 57, no. 4,pp. 2109–2120, 2021.
5. A. Kott, A. Swami, and B. J. West, "The internet of battle things,"Computer, vol. 49, no. 12, pp. 70–75, 2016.
6. T. Chen, S. Barbarossa, X. Wang, G. B. Giannakis, and Z.-L. Zhang, "Learning and management for internet of things: Accounting for adaptivity and scalability," Proceedings of the IEEE, vol. 107, no. 4,pp. 778–796, 2019.
7. S. Russell, T. Abdelzaher, and N. Suri, "Multi-domain effects and the internet of battlefield things," in MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM), pp. 724–730, IEEE, 2019.
8. C. Drubin, "Air force, navy, army conduct first'real world'test of abms.," Microwave Journal, vol. 63, no. 2, 2020.
9. P. Rutravigneshwaran and G. Anitha, "Security model to mitigate black hole attack on internet of battlefield things (iobt) using trust and k-means clustering algorithm," International Journal of Computer Networks and Applications, vol. 10, p. 95, 2023.
10. M. J. Farooq and Q. Zhu, "On the secure and reconfigurable multi-layer network design for critical information dissemination on the internet of battlefield things (iobt)," IEEE Transactions on Wireless Communica- tions, vol. 17, no. 4, pp. 2618–2632, 2018.
11. N. Singh, D. Data, J. George, and S. Diggavi, "Sparq-sgd: Event- triggered and compressed communication in decentralized optimization," IEEE Transactions on Automatic Control, vol. 68, no. 2, pp. 721–736, 2022.
12. C. A. Kamhoua, L. L. Njilla, A. Kott, and S. Shetty, Modeling and design of secure internet of things. John Wiley & Sons, 2020.
13. L. Zhu, S. Majumdar, and C. Ekenna, "An invisible warfare with the internet of battlefield things: a literature review," Human behavior and emerging technologies, vol. 3, no. 2, pp. 255–260, 2021.
14. C. A. Joslyn, L. Charles, C. DePerno, N. Gould, K. Nowak, B. Prag- gastis, E. Purvine, M. Robinson, J. Strules, and P. Whitney, "A sheaf theoretical approach to uncertainty quantification of heterogeneous ge-olocation information," Sensors, vol. 20, no. 12, p. 3418, 2020.
15. S. Yao, Y. Zhao, A. Zhang, S. Hu, H. Shao, C. Zhang, L. Su, and T. Abdelzaher, "Deep learning for the internet of things," Computer, vol. 51, no. 5, pp. 32–41, 2018.
16. S. Joshi, A. Thakar, and C. Patel, "Applications of machine learning and deep learning in securing internet of battlefield things: A futuristic perspective," in 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom), pp. 333–338, IEEE, 2023.