eISSN: 3108-0723

International Journal of Technology, Health and Sustainability

Internet of Military Things (IoMT): Enhancing Situational Awareness and Operational Efficiency in Modern Armed Forces

Nidhi Gour[1*], Kavita Singh[2], Priyanjali Goswami[3], Shantanu Kushwah[4], Madhuri Singh[5]

[1,2,5]Assistant Professor, Applied Science, Sagar Institute of Research & Technology, Bhopal, India.
[3,4]Student, Department of Electronics and Communication, Sagar Institute of Research & Technology, Bhopal, India.
*Corresponding Author

(Received: 04.05.2026; Accepted: 29.05.2026)

Abstract

Technology has significantly optimized the defense sector by enhancing operational efficiency, securing critical infrastructure, and strengthening combat capabilities. Advanced technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), block chain, *cybersecurity, and robotized systems have transformed modern warfare, reconnaissance, and military logistics. IoT-based sensors and connected devices enable real-time data collection from battlefields, borders, and strategic assets. These smart sensors monitor troop movements, environmental conditions, equipment performance, and potential threats. Surveillance drones integrated with IoT systems provide continuous operational monitoring, transmitting live video and intelligence to command centers. This constant data flow improves situational awareness, faster decision-making, and coordinated responses. AI processes vast amounts of collected data to identify patterns and predict risks, while* block chain *ensures secure communication and data integrity. Cybersecurity protects defense networks from cyber attacks. Meanwhile, robotic systems reduce human exposure to danger during reconnaissance and combat missions. Together, these technologies create a highly responsive, data-driven defense ecosystem that enhances mission success and national security.*

Keywords: *Internet of Things (IoT); Machine-to-Machine; Combat capabilities, Internet connected; Internet of military things (IoMT); Automatic chemical agent detection and alarm (ACADA); Chemical, biological, radiological, and Nuclear (CBRN)*

INTRODUCTION

IoT in defense indicates the relationship between devices, sensors, and Tools to improve awareness of surroundings, efficiency, and Resolution. (Atzori *et al.*, 2010). When integrated, these technologies establish an intelligent, protected, and automated security framework. IoT collects, acquires, captures, retrieves, amasses, compiles, or aggregates data and information (Rayes and Salam, 2019). A comprehensive survey of IoT topics and trends further highlights its transformative potential across sectors, including defense (Whitmore *et al.*, 2015).

Additionally, modernized weaponry, hypersonic missiles, laser defense technologies, and electromagnetic spectrum warfare tools have significantly enhanced military capabilities. These technologies mitigate human risk, sharpen precision, and improve operational effectiveness, making defense forces more robust and equipped for modern challenges (DoD, 2022a). The consolidation of these encourages innovation, a more versatile, secure, and technologically advanced defense infrastructure, influencing the future of global defense plans.

Why it Matters

The Internet evolved from the defense domain. In the decades of the 1970s and 1980s, DARPANet, the US Defence Advanced Research Projects Agency Network, utilized switching and protocols to enhance the resilience of communication networks during the Cold War. The military uses Network Centric Warfare and Network Enabled Capability (NEC) to connect soldiers and equipment into a larger system, enhancing synchronization. However, cyber threats delay growth. IoT helps the military by implementing sensors across sea, land, air, and space to accumulate real-time readings. In urban combat, millions of detectors improve situational awareness, enhancing commanders' situational awareness for optimal operations.

IOT INTEGRATION IN DEFENCE

IoT has earlier interrupted many industries with its M2M (Machine-to-Machine) devices architecture or standalone existence in the autonomous system network of devices. Many nations are seeking to leverage IoT in armed forces and defense systems to address various combat and battleground challenges. The Internet of Military Things (IoMT) is a class of IoT for intelligent warfare and modern combat operations. By building a small system of smart technology that can gather sensory information and manage multiple tasks on its own at the same time, the IoMT is conceptually designed to reduce the physical and mental stress that soldiers face during battles. IoMT mainly focuses on and tries to fix the following defense challenges.

The evolution of the Internet of Things (IoT) from machine-to-machine (M2M) communication architectures into fully autonomous, interconnected cyber-physical systems has significantly transformed industrial sectors, and its adaptation into defense has led to the emergence of the Internet of Military Things (IoMT). IoMT refers to a networked ecosystem of smart sensors, wearable devices, unmanned systems, vehicles, weapons platforms, and command systems that collect, transmit, and analyze real-time battlefield data to support intelligent warfare and modern combat operations. According to the U.S. Department of Defense Digital Modernization Strategy (DoD, 2019), integrating connected devices, AI, and secure communications enhances situational awareness, decision superiority, and operational efficiency in contested environments. IoMT systems are conceptually designed to reduce the physical and cognitive burden on soldiers by enabling automated surveillance, health monitoring wearables, smart helmets, autonomous drones, and AI-assisted decision support systems. These systems address key defense challenges such as real-time situational awareness, secure battlefield communication, predictive equipment maintenance, logistics tracking, cyber-physical security, and rapid threat detection. Cybersecurity standards such as the National Institute of Standards and Technology Cybersecurity Framework (NIST, 2018) and SP 800-82 guidelines for Industrial Control Systems (NIST, 2015) further support the secure deployment of connected military infrastructure. Additionally, research initiatives from the Defense Advanced Research Projects Agency (DARPA) of the United States of America contribute to resilient autonomous systems, distributed sensing networks, and secure tactical communications, reinforcing the role of IoMT in reducing battlefield uncertainty while improving operational resilience and soldier survivability (DARPA, n.d.).

Automated Based

Automated bases are military bases that use advanced technology like sensors and internet-connected devices to keep track of important infrastructure in real-time. This helps in better security, maintenance, and efficient management of resources. like power and water systems, and other security-related data monitoring to ensure safety and security.

Automated military bases rely on digital modernization, cyber-physical systems, and resilient infrastructure frameworks supported by official defense and cybersecurity standards. The U.S. Department of Defense outlines smart installation and digital transformation goals in its Digital Modernization Strategy (DoD, 2019) and subsequent energy and water resilience policies, emphasizing real-time monitoring, data integration, and secure networked infrastructure. Cybersecurity and industrial control system protection guidelines are provided by the National Institute of Standards and Technology through its Cybersecurity Framework (NIST, 2018) and Guide to Industrial Control Systems (SP 800-82 Rev. 2) (NIST, 2015), which address SCADA systems, IoT security, and critical infrastructure defense. Challenges to defense infrastructure resilience, including cybersecurity risks, are further discussed by the U.S. Government Accountability Office (GAO, 2022). Research initiatives from the DARPA further contribute to resilient cyber-physical systems and autonomous security technologies (DARPA, n.d.). Additionally, modernization and energy resilience efforts led by the U.S. Army Corps of Engineers (USACE, 2020) support the deployment of microgrids, smart energy management systems, and infrastructure optimization across installations. Academic studies such as Lee *et al.* (2015) on Industry 4.0 cyber-physical architecture and Boyes *et al.* (2018) on the Industrial Internet of Things (IIoT) provide theoretical foundations for predictive maintenance, real-time monitoring, and intelligent infrastructure management applicable to automated military bases.

Asset Tracking

In military operations, effective logistics management is critical because large volumes of weapons, armored vehicles, ammunition, communication equipment, medical supplies, and food must be tracked, maintained, and securely distributed across multiple locations. Traditional manual inventory systems often face challenges such as delayed updates, data inaccuracy, and security risks. The adoption of IoT-based technologies—particularly RFID (Radio Frequency Identification) tracking and smart sensors—has significantly improved real-time asset visibility and logistics efficiency. RFID tags attached to weapons, containers, and supply units allow automated identification and tracking throughout warehouses, transport vehicles, and deployment zones, providing commanders with accurate, up-to-date stock information. According to the U.S. Department of Defense's logistics modernization initiatives, digital tracking systems enhance supply chain transparency and operational readiness (DoD, 2022b). Additionally, smart sensors embedded in combat equipment such as armored vehicles and weapons systems can monitor parameters like temperature, vibration, fuel levels, and mechanical stress, enabling predictive maintenance and reducing unexpected equipment failure. Cyber security and secure data-sharing practices aligned with standards from the National Institute of Standards and Technology (NIST, 2018) ensure that sensitive logistics information remains protected from cyber threats. The U.S.

Government Accountability Office (GAO) has also identified the need for improved asset visibility and accountability in defense inventory (GAO, 2021). Research and innovation programs supported by the DARPA further contribute to resilient, autonomous logistics networks (DARPA, n.d.). Overall, integrating RFID and smart sensor technologies into military supply chains improves accuracy, reduces waste, enhances equipment readiness, and strengthens secure decision-making in defense operations.

Soldiers Health Monitoring Using IOT

IoT sensors can be added to wearable devices, turning them into smart wearables for defense personnel. These devices can track a soldier's health and movements in real time, even from a distance. This helps with instant communication and improves their safety.

Integrating Internet of Things (IoT) sensors into wearable devices transforms them into advanced smart wearables that significantly enhance the operational effectiveness and safety of defense personnel. These systems typically incorporate biometric sensors such as heart rate monitors, body temperature sensors, blood oxygen (SpO_2) trackers, ECG modules, and hydration sensors to continuously assess a soldier's physiological condition in real time. Motion-based sensors, including accelerometers, gyroscopes, and GPS modules, enable precise tracking of location, posture, fall detection, and movement patterns across challenging terrains. The collected data is transmitted securely through wireless communication networks to centralized command systems, allowing remote health monitoring, rapid medical response, and improved situational awareness on the battlefield. By leveraging edge computing and cloud-based analytics, anomalies such as fatigue, heat stress, injury, or irregular vital signs can be detected instantly, enabling timely intervention. Moreover, IoT-enabled smart wearables facilitate seamless communication between soldiers and command units, supporting coordinated operations and mission planning. According to Gubbi *et al.* (2013), IoT frameworks enable interconnected sensing and data exchange systems that enhance real-time decision-making. Similarly, Patel *et al.* (2012) highlight the critical role of wearable sensors in continuous health monitoring and remote supervision. In defense applications, these technologies contribute to improved soldier survivability, operational readiness, and mission efficiency while reducing response time during emergencies.

Shipment Tracking and Management

For any successful military operation, it is important to manage the vehicles that transport soldiers, weapons, and supplies. IoT-based shipment tracking solutions help. Monitor the movement of goods from the starting point to the destination. These systems use sensors and GPS to provide real-time updates on location, temperature, and other conditions, ensuring safe and efficient delivery. IoT devices installed on shipment vehicles help track important details like location, fuel usage, damage, and overall vehicle. For any successful military operation, effective management of the vehicles that transport soldiers, weapons, and supplies is critical, and IoT-based shipment-tracking solutions play a pivotal role in enabling that capability. These systems use GPS and a network of connected sensors to monitor the movement of goods and vehicles from the point of origin to the destination, providing real-time updates on precise location, environmental conditions (such as temperature and humidity), and operational metrics throughout the journey. By equipping military transport vehicles with IoT devices — including GPS trackers, telemetric units, and condition monitoring sensors — commanders and logistics planners can gain continuous situational awareness of fleet movements, fuel usage, engine health, and other key parameters, which helps to optimize routes, prevent breakdowns, and ensure mission readiness. Real-time tracking and telemetrics also support predictive maintenance by alerting when vehicle components deviate from normal performance, reducing the risk of unexpected failures during critical operations. Furthermore, integrated IoT shipment tracking enhances security by offering alerts for route deviations or tampering and supports end-to-end supply chain visibility so that logistics decisions are data-driven and timely. A real-world example of this in the defense sector can be seen in an IoT shipment tracking deployment by an Indian defence organization, where IoT sensors were used to capture GPS location, orientation, and environmental data throughout transit, and an accompanying dashboard delivered real-time insight from material loading to delivery, increasing transparency and reducing the potential for damage or loss.

Battlefield Monitoring

The Internet of Things (IoT) helps track and monitor data in real-time without human involvement. In the military, IoT allows battlefield monitoring using drones with smart cameras and sensors. These drones gather information from the battleground, helping the team keep an eye on the situation and make quick decisions.

IoMT: Revolutionizing Military Operations

Every country works to make its military stronger by using the latest technology and skills. Powerful nations like the USA, Russia, India, and China already have advanced technology to support their defense systems. Now, because of this, using the IoT (Internet of Things) in defense is not just a choice but a necessity.

The Internet of Military Things (IoMT) is a new technology that uses the Internet of Things (IoT) in defense and military. operations. It helps improve situational awareness, decision-making, and remote monitoring of military assets.

In simple terms, IoMT connects military equipment like helmets, weapons, and vehicles using sensors and smart technology. These devices can communicate with each other and share data over the internet, helping the military to track, analyze, and respond quickly in different situations.

MODERN EQUIPMENT USES IN THE INDIAN ARMY

ACADA means Automatic Chemical Agent Detection and Alarm System. It is an important tool used by the Indian Army to quickly find harmful chemical agents in the air and give a warning. This helps protect soldiers from Chemical, Biological, Radiological, and Nuclear (CBRN) threats and keeps them safe during dangerous situations.

The ACADA is an advanced defence-oriented detection system whose primary function is to identify the presence of Chemical Warfare Agents (CWAs) and pre-programmed Toxic Industrial Chemicals (TICs) in the air, enabling rapid warning and response to chemical threats. Developed indigenously by the Defence Research and Development Organisation (DRDO) (PIB, 2025), ACADA continuously samples ambient air and uses Ion Mobility Spectrometry (IMS) technology with highly sensitive cells to detect and simultaneously monitor a wide range of hazardous chemical agents — including nerve, blister, blood, and choking agents — at low concentrations. Upon sensing dangerous substances, the system immediately triggers both audible and visual alarms, alerting military personnel to take protective actions, and can also be networked with central monitoring stations for broader area surveillance. This capability ensures that chemical hazards — whether from deliberate use in warfare or accidental industrial releases — are detected promptly, enhancing the safety and operational readiness of forces deployed in both combat and peacetime environments.

Detection of Chemical Threats

The main function of ACADA is to detect the presence of chemical warfare agents (CWAs) and planned toxic industrial chemicals (TICs) in the air. These are hazardous substances that can be used in chemical attacks or released during industrial accidents.

Early Warning System

ACADA quickly and continuously checks the environment and gives instant audio and visual alarms. This early warning helps people put on protective gear in time and allows leaders to start defense actions. This way, it helps reduce injuries and keeps operations running smoothly.

CBRN Defence

ACADA is an important part of the Indian Army's plan to protect soldiers and equipment from dangerous threats like chemicals, germs, radiation, and nuclear attacks.

Ways to Enhance the ACADA System

ACADA detects toxic chemicals due to their molecular structure and ions of the chemical. But sometimes it fails to determine the ions' mobility of toxic substances because the chemicals in the environment have similar ion mobility to the target agent. To avoid this problem in ACADA, we use detectors based on Artificial intelligence technology and input the instructions related to the Basic Neurological science of the molecular structure of the toxic chemicals that harm the environment.

Environmental Factors

ACADA performance can be affected by environmental conditions such as extreme temperatures, humidity, and dust, which impact the efficiency of air sampling and detection. To avoid these environmental factors, ACADA material is made of a highly rigid material that resists all environmental factors. Materials are made that have high thermal expansion, and they resist temperature factor and work in extreme locations.

Challenges in IOT Adoption

- Cybersecurity threats due to connected gadgets.
- Data deluge and the need for instantaneous computation (Kumar *et al.*, 2019).
- Network flaws in a hostile environment.

Research Analyses and Current Implementations

- U.S. Military IoT Projects
- Indian Defense IoT Initiatives
- Israel's Smart Defense Systems

CONCLUSION

The use of IoT technology in the military is being developed to improve combat effectiveness and manage resources more efficiently using large amounts of data. The accuracy and reliability of this data are crucial for making good military decisions. However, the current systems for transmitting and processing battlefield information are not advanced enough to meet modern and future needs. That's why IOBT (Internet of Battlefield Things) has become important in defense applications, as it helps in better data collection, faster communication, and smarter decision-making.

When all data flows into one central system, that system and its communication links become prime targets for cyberattacks. The Internet of Things technology allows machines to act in the real world using smart controls. This helps in managing operations in the air, on land, at sea, and even in space using digital systems. Since a huge amount of data needs to be transferred, strong communication networks are necessary to support command and control (C2) systems. Researchers are now looking into moving beyond 5G networks and exploring the potential of 6G technology.

With IoT and an intelligent C2 system a, military commanders can get the information they need to quickly adjust their forces and resources when facing unexpected challenges, like losing equipment or dealing with difficult terrain and bad weather. To make this work, changes will be needed in military strategies, tactics, and unit structures. This is a critical domain for ongoing and advanced research.

Grant Support Details

The present research did not receive any financial support to conduct the research.

Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of this manuscript. In addition, the ethical issues, including plagiarism, informed consent, misconduct, data fabrication and/ or falsification, double publication and/or submission, and redundancy has been completely observed by the authors.

REFERENCES

1) Atzori, L., Iera, A. and Morabito, G. (2010) 'The Internet of Things: A survey', *Computer Networks*, 54(15), pp. 2787-2805. https://www.sciencedirect.com/science/article/pii/S1389128610001568

2) Boyes, H., Hallaq, B., Cunningham, J., *et al.* (2018) 'The industrial internet of things (IIoT): An analysis framework', *Computers in Industry*, 101, pp. 1-12. doi:10.1016/j.compind.2018.04.015.
3) DARPA (n.d.) Defense Advanced Research Projects Agency, U.S.A. https://www.darpa.mil/
4) DoD (2019) *Digital modernization strategy*. Washington, DC: U.S. Department of Defense. https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF
5) DoD (2022a) *National defense strategy of the United States of America*. Washington, DC: U.S. Department of Defense. https://media.defense.gov/2022/Mar/28/2002964702/-1/-1/1/NDS-FACT-SHEET.PDF
6) DoD (2022b) *DoD Supply chain materiel management procedures (DoDI 4140.01)*. Washington, DC: U.S. Department of Defense. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/414001p.pdf
7) GAO (2021) *Defense inventory: Actions needed to improve asset visibility and accountability*. GAO-21-108. Washington, DC: U.S. Government Accountability Office. https://www.gao.gov/products/gao-21-108
8) GAO (2022) *Defense infrastructure: Resilience and cybersecurity challenges*. GAO-22-105. Washington, DC: U.S. Government Accountability Office. https://www.gao.gov/products/gao-22-105
9) Gubbi, J., Buyya, R., Marusic, S., *et al.* (2013) 'Internet of Things (IoT): A vision, architectural elements, and future directions', *Future Generation Computer Systems*, 29(7), pp. 1645-1660. doi:10.1016/j.future.2013.01.010.
10) Kumar, S., Tiwari, P. and Zymbler, M. (2019) 'Internet of Things is a revolutionary approach for future technology enhancement: a review', *Journal of Big Data*, 6, 111. doi:10.1186/s40537-019-0268-2.
11) Lee, J., Bagheri, B. and Kao, H.A. (2015) 'A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems', *Manufacturing Letters*, 3, pp. 18-23. doi:10.1016/j.mfglet.2014.12.001.
12) NIST (2015) *Guide to industrial control systems (ICS) Security*. SP 800-82 Rev. 2. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r2
13) NIST (2018) *Framework for improving critical infrastructure cybersecurity, Version 1.1*. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018
14) Patel, S., Park, H., Bonato, P., *et al.* (2012) 'A review of wearable sensors and systems with application in rehabilitation', *Journal of NeuroEngineering and Rehabilitation*, 9(21). doi:10.1186/1743-0003-9-21.
15) PIB (2025) *Indian Army procures critical CBRN defence equipment*. Press Information Bureau Delhi. Release ID: 2106362. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2106362
16) Rayes, A. and Salam, S. (2019) *Internet of things from hype to reality: The road to digitization*. 2nd edn. Cham: Springer. https://doi.org/10.1007/978-3-319-99516-8
17) USACE (2020) *Engineering and construction bulletin: Energy resilience and conservation investment program (ERCIP)*. Washington, DC: U.S. Army Corps of Engineers. https://www.publications.usace.army.mil/Portals/76/Publications/EngineerBulletins/EB_2020-03.pdf
18) Whitmore, A., Agarwal, A. and Da Xu, L. (2015) 'The Internet of Things—A survey of topics and trends', *Information Systems Frontiers*, 17(2), pp. 261-274. doi:10.1007/s10796-014-9489-2.