Investigation and Implication of Advanced Sensory Computing in Military and Defense Applications

Debasis Nayak[1], Ishan Ganguly[2] , Sushruta Mishra[3] and Kunal Anand[4]

[1,2,3,4] *Kalinga Institute of Industrial Technology, deemed to be University, India*

Abstract

This research paper explores the various applications of the Internet of Things (IoT) technology in the defence sector. The Internet of Things (IoT) and the development of defence technologies are both topics covered in this paper. IoT is now seen as a path-breaking technology that has the potential to reshape a number of industries, including the defence industry. The term "Internet of Things" (IoT) describes the networked interconnection of physical entities, including machinery, infrastructures, and other things, that are equipped with sensors, applications, and inter-networking. For defence organizations, the potential of IoT to collect, analyze, and distribute data in real-time presents enormous opportunities to improve situational awareness, decision-making abilities, and operational efficiencies. The study centers on the utilization of smart units and sensory modules to improve combat tactical awareness, logistics and supply chain management, and military hardware predictive repair. Several case studies are provided in the paper to demonstrate these uses, including the use of autonomous aerial vehicles (UAVs) for real-time data gathering, IoT devices for monitoring equipment and people movement, and predictive repair for increasing operational availability. The study finds that the use of IoT technology in defense has the potential to greatly improve military operations by allowing leaders to make better choices based on real-time data and increasing total combat efficiency and efficacy. The paper emphasizes the significance of real-time data gathering and analysis in the military context, as it enables commanders to make informed choices swiftly and react to rapidly shifting battlefield conditions. The usage of smart approach in logistics and supply chain management guarantees that crucial resources are in the right location at the right moment, improving total operational efficiency.

Keywords
Internet of Things, Defense technology, Cybersecurity, Surveillance, Smart computing, Data privacy.

1. Introduction

Network centrality has significantly changed military strategy and war fighting since the final period of the twentieth century. The Internet of Things (IoT), the next rung on the networking scale, has already begun to fundamentally alter how society operates by connecting a vast number of intelligent devices that are interconnected and capable of communicating with one another. IoT is expected to proliferate at a similar rate in the military in the near future, which will fundamentally alter how they operate and conduct operations. This paper examines various aspects and provides an evaluation of the IoT centrality of futuristic defense activities

SCCTT 2023: Proceedings of CEUR Workshop Proceedings, Month 07–12-2023, New Delhi, India

2005653@kiit.ac.in (Debasis Nayak); 2005659@kiit.ac.in (Ishan Ganguly); sushruta.mishrafcs@kiit.ac.in (Sushruta Mishra); kunal.anandfcs@kiit.ac.in (Kunal Anand)
0000-0003-3929-1100 (Sushruta Mishra); 0000-0003-0316-3502 (Kunal Anand);

driven by IoT idea, obstacles and evolutionary paths of major power. Recent studies [1] have discussed about IoT and their vital utilization in military domain. The use of sensors in work zone may enhance military authorities' situation based alert level, risk management, and execution delay. IoT-based solutions can help the military detect the adversaries, keep track of the physical and mental health of the armed personnel, and coordinate the armed personnel with defence systems. Armed personnel's positions and vital signs can be obtained using military outfits and helmets with embedded sensor devices. To protect life of defense staffs, the command center has the ability to respond immediately. Some of the sensors that can be utilized to create intelligent military gear are the climatic sensor, heart sensor, accelerometer, ECG sensor, mobility sensor, and oxygen level sensor.

Connecting devices and objects to the internet enables them to gather and share data in real-time. This technology trend is denoted as the "Internet of Things" (IoT). IoT is being used in the defence sector to build smarter, more interconnected systems that can help boost situational awareness, increase communication, and improve decision-making. In order to secure a nation’s defense sector, its military unit should be efficient. Army staffs who are on war zone or who are allotted any special task are going to be benefited from this. As discussed by Sujitha, v et al. [2] GPS would be used to track the soldiers' whereabouts, well-being, and other details (Global Positioning Systems). Mobile Medicare approaches, including robust computing devices, clinical sensors, and transmission methodologies, are used to continuously monitor the health of troops from a distance. Smart sensors including temperature and heart rate sensors, as well as bomb detectors and panic buttons, are coupled to the suggested system, which will use a personal server to accomplish full mobility. The CPU receives the parameters gathered by the real-time sensors attached and processes them further. Internet of Things (IoT) is emerging as a quickly adapting concept which leads to fast and reliable information transfer. Several countries are unable to monitor events leading to any casualty of staffs regardless of any alert or prior data securing. The lives of war fighters cannot be replaced, so it is important to protect their lives. Controlling military ammo is a crucial and essential aspect of military operations. The creation of intelligent military tools is a significant application of IoT in the defence sector. This covers everything from drones and tanks to smart weapons and military equipment. In their work Utsav, A et al. [3], have proposed internetworking models on basis of IoT for military applications. There are several geographical areas that the military is unable to monitor and detect any unauthorized signal or activity. To make things simpler and so that their system can locate a specific place wherever surveillance is required. They allocated a number of different UAV networks for the surveillance of the area and for security-related monitoring. Armed forces personnel can gather up-to-the-second information about their surroundings, and possible threats by integrating these devices with IoT sensors and connectivity.

In [4], various radio frequency detection modules, cameras, sensory units, positioning units and other perception interfaces are discussed in context to military tasks. Networking interface is responsible for routing packets from perception interface to the application interface facing various constraints in network. Smart systems make use of small range-based network transmission methods like Bluetooth and Zigbee to forward signals from perception interface to routers on basis of abilities of transmitting entities. Networking techniques like 3G and 4G or any energy communicative line can route data over long route distance. As, applications intend to develop smart environment, this will boost the creation of smart military facilities, which is another use of IoT in defence. These bases have a network of sensors and other connected devices that can track everything from security and surveillance to electricity and water use. Military leaders can optimize operations, boost security, and cut expenses by gathering and analyzing this data. While the use of IoT in defense technology offers several benefits, there are also some cons that need to be considered. One of the primary concerns is the cybersecurity risks associated with IoT. Das, M L et al. [5] have discussed IoT security and privacy concerns would be far more difficult to address than they are in traditional wireless contexts. To ensure that IoT takes on the intended form, restricted contexts in particular call for lightweight primitives, secure design, and efficient embedding into other settings. With a focus on the security goals and privacy requirements for resource-constrained contexts, also examined secure authenticity issues in smart use cases in the article. IoT devices are susceptible to hacking, and a security lapse on their part might have grave repercussions. Defense organizations deal with highly sensitive information, and a security breach could compromise the safety of troops and compromise national security. There are concerns about the privacy of personnel who are required to use IoT devices. Wearable and other IoT devices may collect personal information about the user, and there is a risk of this information being misused or hacked.

This study explores the impact of the Internet of Things (IoT) on defence technology, focusing on its role in improving situational awareness, communication, and decision-making in military operations. It will analyze case studies and literature to assess its advantages, challenges, and future prospects. The study aims to contribute to ongoing discussions on IoT's application in defense technology and offer a framework for weighing its advantages and disadvantages. Challenges include cybersecurity risks, interoperability issues, the need for reliable network infrastructure, and privacy concerns.

2. Related Work

Atul Pant et al. [6] provides a comprehensive overview of the potential of IoT technology in shaping the future of military operations. The author highlights the potential benefits of IoT technology in enhancing situational awareness, improving communication and coordination, and optimizing resource management. However, the author also notes that there are significant challenges associated with the implementation of IoT technology, including cybersecurity risks and interoperability issues. The author emphasizes the importance of a coordinated and collaborative approach to the development and implementation of IoT technology in military operations, and highlights the need for strategic planning and investment in research and development to ensure that the full potential of IoT technology is realized in the future of military operations.

Vishal Gotarane et al. [7] emphasizes the importance of real-time data collection and analysis in military operations, and explains how IoT-enabled devices can provide valuable data on troop movements, equipment status, and other critical information. The work also explores various applications of IoT technology in military operations, including surveillance and reconnaissance, logistics and supply chain management, and battlefield healthcare.

Martinez-Caro, J.-M. et al. [8] note that the integration of IoT technology in unmanned systems, such as drones and autonomous vehicles, can improve their capabilities in terms of sensing, decision-making, and communication. The paper highlights the potential of IoT-enabled drones for reconnaissance, surveillance, and target acquisition, and how they can be used to gather real-time data on enemy positions and movements. The author also cover how IoT can be used to improve the powers of smart weapons.

Ninad V. Joshi et al. [9] discusses the deploy and implementation of an IoT driven sensory vest and helmet for the defense sector. The smart vest and helmet are designed to provide various features such as real-time monitoring of vital signs, GPS tracking, and communication capabilities. The vest and helmet consist of various sensors and devices such as a heart rate sensor, a temperature sensor, a GPS module, a micro-controller, and a communication module.

Iyer, Brijesh et a.l [10] in their work on "IoT enabled tracking and monitoring sensor for military applications" Report an IoT-based system for battlefield health surveillance and analysis. The sensory module acts as a cost-effective and accurate alternative for troop surveillance. For determining human life, various human vital indicators and combat circumstances such as body temperature, pulse rate, smoke recognition, and oxygen saturation are used. A distress buzzer is also included, which may be helpful for the solder to summon immediate assistance on the battleground. The new technology described by Eszter Katalin Bognar et al. [11] provides vital growth in various defense zones. The author agrees that the implementation of exploratory data security necessitates a novel approach and points to recent projects in the internetwork army, IoT based medical tracking, driving units, sensory logistics, IoT based defense bases, and embedded intelligent specific analytics units as the initial trend and significant rise in this field are anticipated in the future.

Mariani, Joe et al. [12] provides a comprehensive overview of the Internet of Things (IoT) in the military context. They describe the IoT in the military's historical growth, present condition, and possible future developments and possibilities. The writers' thorough examination of the development of IoT historically and in the context of warfare is one of this paper's strong points. Beginning with the use of radio technology for transmission during World War II, they trace the early evolution of IoT in the military. The growth of IoT in the military context is then described, including the creation of different transmission technologies, the application of unmanned systems, and the appearance of connected devices. Overall, the author offers a thorough analysis of IoT in the military context, covering everything from its historical development to its present state and potential future developments.

In their work Kang, James Jin et al. [13] have proposed a generic energy constrained model for assisting defence staffs in critical events-based tasks. Various military network uses are included in the suggested framework. Health data and biometric for employee identity have been used to improve multi-factor verification. To minimize power usage, multi-layer inference methods were used to increase accuracy and efficiency. The subsequent inference interface enhanced with savings rate of datasets grew while precision got reduced by only 0.9% as compared with the first layer inference algorithm, which had already improved savings and accuracy rates.

Sehrish Mudassar et al. [14] discusses Wireless Sensor Networks (WSN), a branch of the Internet of Things that is a new field of research. A key application field for sensing nodes and IoT has been recognized as military reconnaissance, which is a crucial part of defense and military activities. Link scheduling systems were the subject of a study of the literature. This research focuses on resource scheduling for the military because there isn't a specific scheduling plan discussed in the literature. Additionally, a paradigm for resource scheduling that finds a compromise between competing demands for quality of service for two different traffic groups is created.

Abhishek, R et al. [15] in the work highlights IoT Driven Defence Vehicle System and concentrates on developing a prototype man less ground vehicle with multiple functions. This device can move objects with the help of DC motors. The process makes use of DC gear motors, which are operated at 500 RPM and 12.5 kgcm torque. For various purposes, the prototype is fitted with various sensors, including PIR, Ultrasonic, Temperature, Gas, Accelerometer, and Metal Detector. When explosives are discovered, the robotic arm is used to transfer the items. This man-less ground vehicle is built to operate anywhere in the globe and to perform in hazardous conditions.

Sabarimuthu, M. et al. [16] in their work established private data transmission among army staffs and base node. Poisonous gas attacks could be discovered early with the help of gas sensors. Motion sensors can track the assailants' movements and alert the troops to their whereabouts. Metal items that are concealed inside of other objects can be found using a metal detector. The GPS device also sends the soldier's location information to the base station. When in need, a soldier can press the SOS icon to signal for help from other troops. As a result, the suggested method offers the best option for a system of monitoring and protection for soldiers. The micro-controller is provided a power supply for use in their job. It has a gas monitor that can detect poisonous chemicals. Metal that is hidden beneath is found using a metal detector.

Dhananjay et al. [17] have spoken about the battlefield's health and weapon state control system while keeping deployed troops in mind. The command center (commander) and troops can communicate with each other in both directions using the hierarchical IoT communication design. As a result, the leader can keep an eye on the health of the soldiers (parameters like body temperature, heart rate sensor, blood circulation, sugar levels, ECG levels, etc.) and the condition of the weaponry before making military choices that are important for the army.

Mishra, L. et al. [18] in their work provided a detailed review of the usage of IoT in the defense perspective. Drone-based surveillance is the most important of the mentioned aspects because it detects the presence of intruders or harmful weaponry without the direct participation of humans, providing security to our troops. Furthermore, they have proposed a new idea of smart camps, which is merely a hypothesis. After this theory is implemented, we will be able to detect the presence of intruders and explosives around the camps, preventing an assault and potential devastation.

3. Role of IoT sensors in Defence Technology

The way we engage with technology has been completely transformed by the Internet of Things (IoT). IoT allows things to interact and share data with one another by utilizing sensors and wireless connectivity, leading to the development of smarter, more effective systems. IoT technology has been applied in the military and defense industries to increase situational awareness, decision-making, and operational efficiency. We will talk about the use of IoT sensors in military and security technology in this piece. Figure 1 shows the different applications of IoT in military use cases.

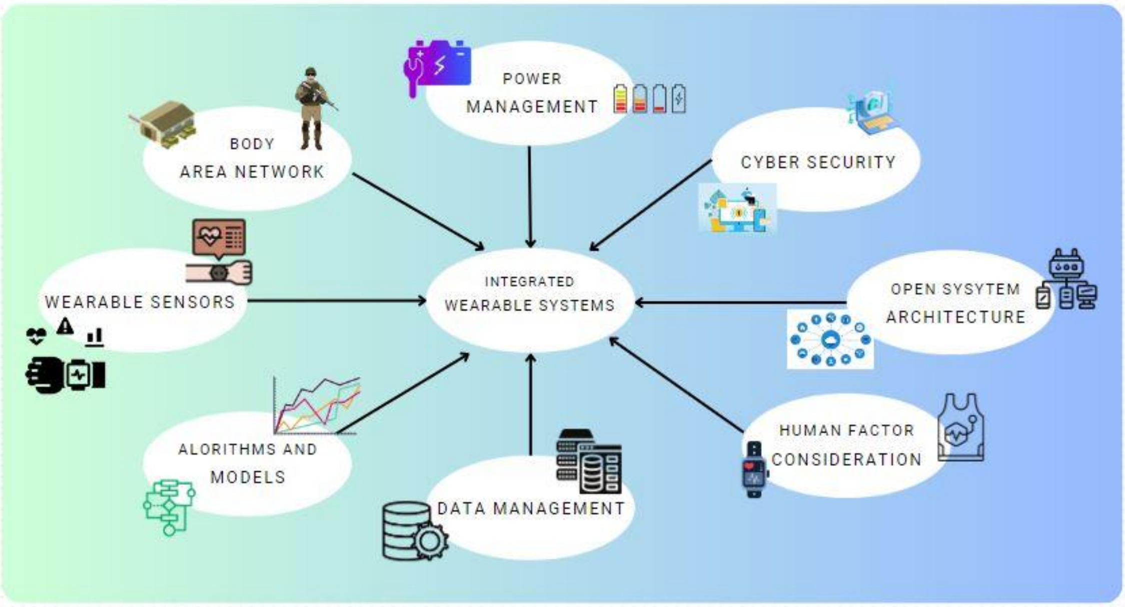

Figure 1: Depiction of IoT application in military

3.1. Awareness of the situation

In the military and security industries, situational alertness is essential. A variety of apps use IoT devices to assist with situational awareness. Unmanned aerial vehicles (UAVs), for instance, use IoT devices to collect real-time information on the positions of enemies, the topography, and the weather. The command center receives this data, which is then examined there to reveal information about the battleground. Additionally, smart helmets donned by troops utilize IoT sensors. These headgears have sensors and cams inside that record information about the surroundings. The information is then real-time processed to give troops a 360-degree picture of their surroundings. By increasing environmental awareness, troops are better able to make choices.

3.2. Prevention-based maintenance

Equipment malfunction can have disastrous consequences in the military and security industry. IoT devices are used in a variety of military hardware, such as ships, tanks, and airplanes, to keep track of the condition of vital parts. IoT sensors can forecast when machinery is likely to malfunction by examining data on component performance. As a result, proactive repair can be carried out by maintenance teams, cutting delay and raising dependability.

3.3. Management of the supply chain and logistics

In the military and security industry, supply chain management and logistics are essential. Real-time monitoring of people, equipment, and supply movements is done with the help of IoT devices. Following an analysis of this data, logistics processes are optimized for cost and productivity savings. IoT devices are also used to keep an eye on the state of goods while they are being transported. For instance, monitors can be installed on shipping crates to track vibration, humidity, and temperature. This guarantees that goods, including medical gear and ammunition, are delivered in the best possible manner.

3.4. Cybersecurity

Cybersecurity is essential in the military and defense industry. Network monitoring and danger detection are carried out using IoT devices. For instance, monitors can be used to track network activity and spot any oddities that might point to an assault. This lowers the possibility of data leaks and hacks by enabling Cybersecurity teams to react rapidly to threats.

Applications for real security, like access control systems, also use IoT devices. Security teams can identify and stop unauthorized entry efforts by using sensors to watch doors and exits. The security and military sectors have been changed by Internet of Things sensors.

4. Different types of IoT sensros in Defence Technology

4.1. Global positioning system (GPS) sensors

GPS sensors are one of the most essential tools in the defense industry. By giving precise, real-time position data, GPS sensors have completely changed how the military conducts business. This information is essential for a variety of military uses, including aiming and guidance. In-depth descriptions of GPS devices and their applications in the defense industry are given in this piece. A circuit model for GPS sensor is shown in Figure 2.

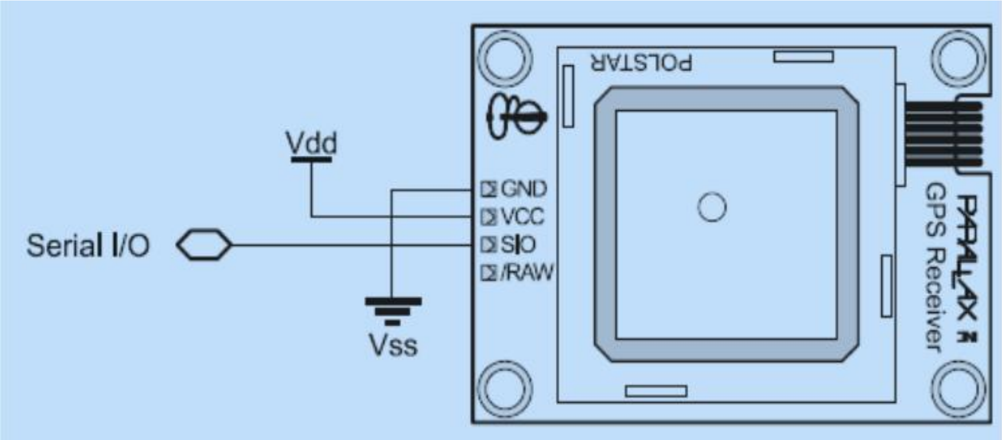

Figure 2: Circuit diagram of GPS sensor

The GPS sensor uses trilateration to determine its distance from each satellite by measuring the amount of time it takes for messages to move from the satellites. The GPS sensor can determine its exact position by adding this distance information to the location data transmitted by the satellites. In the field of defense, GPS devices are used for a variety of tasks, including targeting and guidance. The following are a few of the most significant uses for GPS sensors in the armed forces. Navigation: In the military, GPS devices are frequently used for tracking. Targeting: In the military, GPS devices are also used for aiming. Reconnaissance: In the military, GPS sensors are also used for surveillance. They can be used to follow the movements of hostile forces' soldiers and vehicles, giving crucial information for strategizing military actions. Additionally, friendly troops can be tracked and located using GPS devices to make sure they are working in the proper areas and are not in danger of ambush. Communication: In the military, GPS devices are also used for contact.

4.2. Infrared sensors

Infrared (IR) sensors are crucial in the defense sector for identifying and analyzing the environment through thermal radiation. They are used in both civil and military defense systems, with military systems focusing on tactical and strategic components and civilian defense encompassing homeland security. Despite technical challenges, infrared sensors are desirable due to their passive capabilities, lower bulk and power consumption, and use in all missile defense operations. Nanotechnology offers potential for infrared components with unique material and physical features, advancing rapidly. An infrared sensor is shown in Figure 3.

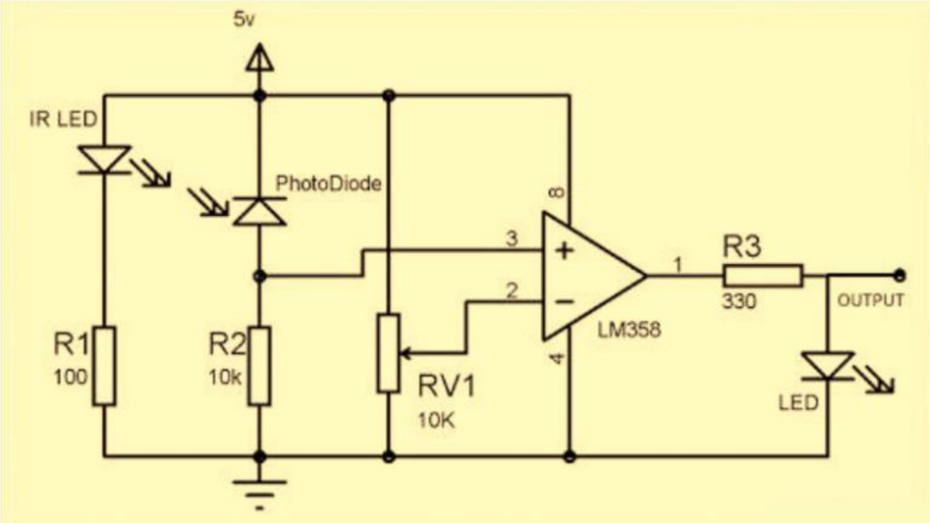

Figure 3: Circuit diagram of infrared sensor

Infrared sensors detect and analyze thermal energy released by objects in their surroundings. These electrical devices consist of a detector, signal generator, and display. The signal processor analyzes data and creates a display for the user. IR sensors come in various forms, including inactive, active, and semi-active ones. Active sensors generate their own infrared radiation and detect reflections, while passive sensors sense infrared radiation from objects. Semi-active sensors emit infrared radiation and sense both emitted and reflected radiation. The effectiveness of IR sensors depends on factors like sensor temperature, substance type, and atmospheric conditions. Other infrared radiation sources, such as sunlight or artificial sources, can also conflict with IR sensors.

4.3. Acoustic sensors

Acoustic sensors are electronic devices designed to detect, measure and analyze sound waves. They are commonly used in the defense sector for various purposes, including detecting and tracking submarines, aircraft, and missiles. These sensors can be deployed on a wide range of platforms, from ships and submarines to airplanes and drones, and can provide valuable information to commanders on the battlefield. The acoustic sensors have helped in designing gun positioning approach with defense alternative as its origin for self-protection tasks and currently it led to intelligent rule-based business policies on demand basis. Basics of gun activities forecasting within muzzle signal projection of super-fast missiles are analyzed. These gun related events are moreover defined in context to sensory captures and its consequences in gun positioning outcome. Figure 4 shows an acoustic sensor model. There are various kinds of acoustic sensors used in the defense sector, including hydrophones, Sonobuoys, acoustic arrays, and acoustic cameras.

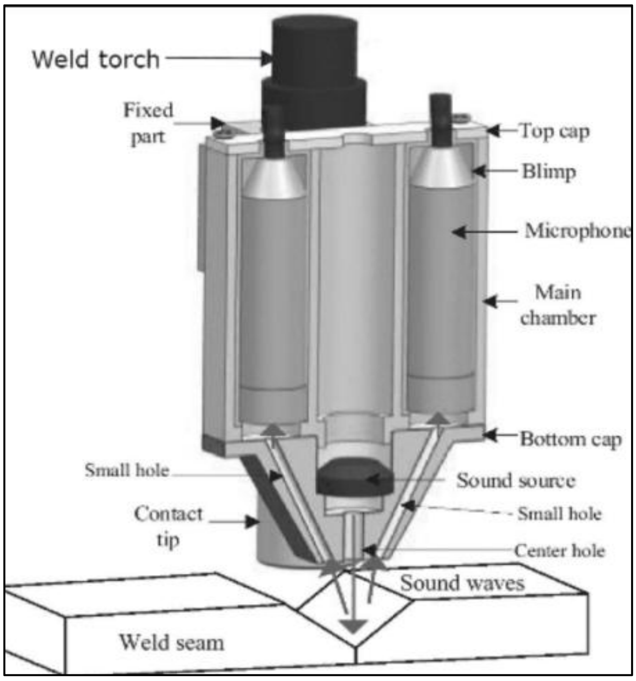

Figure 4: Depiction of acoustic sensor model

4.4. Optical sensors

Electronic tools called optical sensors are created with the purpose of detecting and measuring light or electromagnetic waves. They function by reacting to variations in the brightness, wavelength, or polarization of light and have a variety of uses, such as environmental tracking, process management in industry, and medical diagnoses. Optical sensors are a crucial piece of equipment used in the military and defense industry for a number of tasks, such as locating and recognizing targets, following and directing weapons, and giving military people situational awareness. A sample ray diagram of an optical sensor is shown in Figure 5.

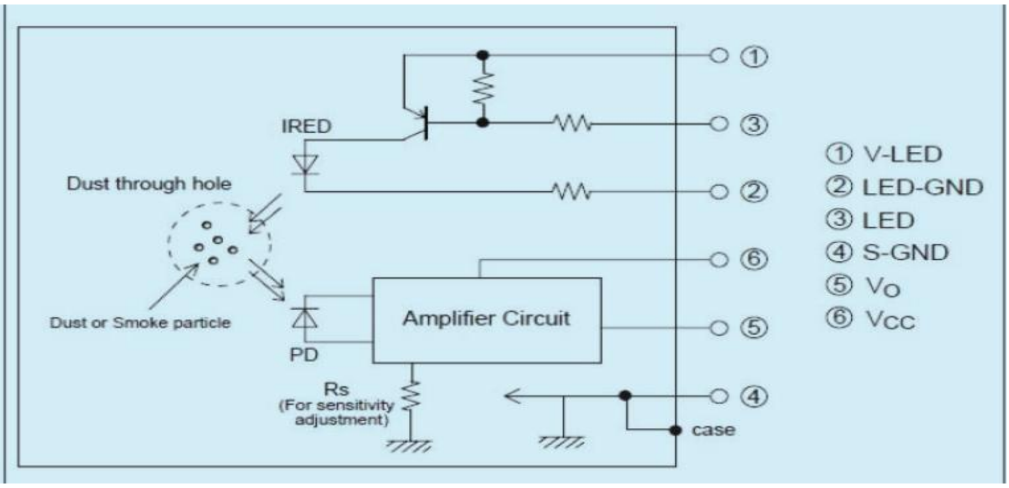

Figure 5: Ray diagram for optical sensor

Optical sensors can typically sense light in a specific electromagnetic spectrum, such as the visible, infrared, and ultraviolet ranges. The photoelectric effect is used by this sensor to easily identify the polarization of light, wavelength, or frequency and convert it into an electric signal. The primary determinant of an optical sensor's detecting principal is a shift in the properties of the optical signal. Since light is primarily used as the carrier in this sensor's operation, its sensing range is very broad. Transmitter (also known as an optical source) and receiver are the two basic parts of optical detection. (optical detector). Any item that gets between the transmitter and receiver causes the light beam's characteristics to shift. In optical detection, the five important properties of light—intensity, phase, wavelength, polarization, and spectral distribution—are detected.

5. Different types of IoT sensors in Defence Technology

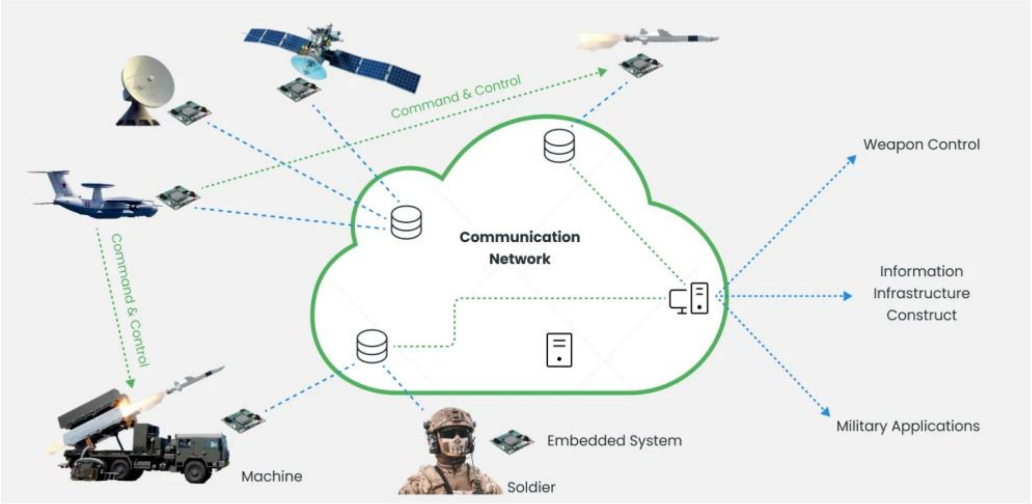

Figure 6: Depiction of application of IoT in military for communication

As you can see in Figure 6, IoT military smart devices significantly contribute to troop lifesaving. However, a sophisticated system like this can only function continuously if there is continual and uninterrupted communication between all of the connected components, including soldiers, warehouses, trucks, equipment, operators, and the command centre. Breaking the connection between its components might decrease efficiency or possibly render it inoperable because all of its pieces must operate as a single complex system. Wire transmission was the most reliable and unbroken form of data transmission for many years, yet for contemporary combat operations, such a technology is not only obsolete but also impractical. Today, the majority of other biometric data is transmitted using encrypted radio transmission, much like regular IoT.

In order to aid in their tactical planning, live simulation is used as shown in Figure 7. That is, real humans run real instrumented devices, and only the impacts of the weapon appear emulated. The drills may affect each sub-team, mix activities and events, and expose the master' abilities. The replay and post-action evaluation of actor decisions and person acts are also essential lessons for improving actor response. In this situation, the vertices of the tetrahedron correlate to the following live simulation actors:

- Process: Combat training activities such as injury management, target identification, penalty impacts, and so on. Data from sensors, armed vehicles, tanks, and other devices is combined and evaluated to build quick frameworks and equipment control schedule-based processes. This could aid to enhance system efficiency and general tasks of model.
- Person: Soldiers, unit commandants, operations control center employees, and staffs (group discussions, vehicles prime tenant and clinical facilitator).
- Intelligence based entities: Sensors, actuators, tools, and vehicles capable of producing a precise image of real-time activities in order to allow real-time management. Tactile suits, combined head-based devices, and other intelligent items are examples.
- Technological ecosystem: Sensors, actuators, tools, and vehicles capable of producing a precise picture of real-time activities, allowing for real-time management. Intelligent items may include tactile suits, combined head-based devices, and so on.
- Privacy: seeks to minimize the danger of confidential data disclosure (troop) where shared with a modern environment. Anonymity, encrypted process, aggregated data, amalgam, and synchronized approach are data management methods that can be used to conceal private details while still giving important information for the pertinent usecases.
- Trust: focuses on soft privacy (technical environment) to build reciprocal confidence between intelligent entities and staffs, as well as to provide security assurances and openness during military exercises. As a result, the worldwide system is able to provide timely and trustworthy data where it is required, timing of need, and who will require it. Trust will be established based on two factors: the intelligent object's ability to defend itself against a dangerous environment, and the person's ability to question the node to determine whether it is still trustworthy.
- Identification / Access control: Controlling unauthorized intrusions of persons/objects into limited regions. They may concern the identity and location of ordnance and weapons, the measurement of explosives and poisonous chemicals, the monitoring of troops, the detection of shooters, and the management of surveillance parameters in sensitive areas.
- Reliability: concentrates on the dependability of information gathered and outcomes relayed by the technological ecosystem during the military process. For example, if models do not produce the same stress as a real battle, the impact on the dependability of a virtual simulation is inaccurate, because people react differently when stressed. Furthermore, tools or vehicles may rarely crash because unreliability was not adequately simulated. To compensate for this shortcoming, the simulated equipment behavior may mimic task failure, gasoline usage, or ammunition utilization based on real-world values [19].
- Safety: seeks to satisfy the demand for intelligent objects, guarantee their safety throughout their entire life cycle, and enhance people's safety by decreasing accidents and deaths during activities. In military operations, an attacker may leverage a medical device's weakness, such as cardiac pacemakers or diabetic machines, and kill victims. Another situation is when a combatant is cautioned about dehydration, elevated pulse rate, low blood sugar, and so on. Monitoring tools may allow for an effective health system and/or the provision of health services as needed.

- Auto-immunity: It deals with how to defend intelligent objects from physical assault in highly harsh military operations settings, as well as providing resilience to shock and tremor; with the ability to self-monitor and report. It also concentrates on improving the resistance of intelligent devices and communication routes to disturbance and jamming.

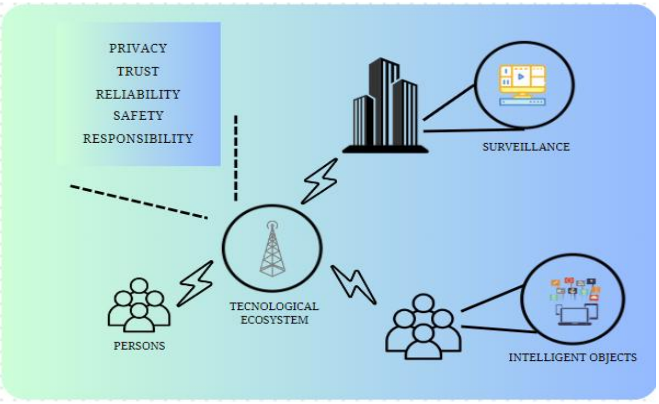

Figure 7: Military life simulation and security issues

6. Challenges of smart sensors deployment in military applications

The paper also discusses the challenges associated with implementing IoT in the military, including:

6.1. Resource security

Implementing IoT devices in defense can bring many benefits, but it also introduces several security issues that need to be addressed. Some of the significant security issues in implementing IoT devices in defense are:

- Data Security: IoT devices gather sensitive information and transmit it over the network, which can be intercepted by hackers. Unauthorized access to such information can be disastrous and compromise national security.
- Device Security: IoT devices can be physically tampered with, allowing the attacker to modify or steal information. Therefore, proper device security measures are necessary to prevent unauthorized access [20-21].
- Network Security: IoT devices communicate with each other and with the cloud through networks that can be vulnerable to cyber-attacks. An attacker who gains access to the network can cause significant damage to the defense system.
- Authentication and Authorization: IoT devices require authentication and authorization mechanisms to ensure that only authorized personnel can access them. Failure to do so can lead to unauthorized access to the system.
- Remote Access: IoT devices can be accessed remotely, and remote access can lead to security vulnerabilities. It's essential to limit remote access to authorized personnel only.

6.2. Interoperability

The implementation of IoT devices in defence raises several interoperability issues due to the complex and heterogeneous nature of the defence systems. Some of the key interoperability issues are:

- Compatibility: IoT devices may not be compatible with existing defence systems, making it difficult to integrate them seamlessly. This may require extensive modifications to the existing infrastructure, which can be time-consuming and expensive.

- Privacy: Defence systems must be highly secure and protected from cyberattacks. IoT devices may not have the same level of security, which can make them vulnerable to attacks and compromise the entire system [22].
- Data integration: IoT devices generate large volumes of data, which must be integrated with existing defence systems. This can be challenging because the data generated by IoT devices may be in different formats and require different protocols for processing and analysis.
- Scalability: Defence systems are large and complex, and IoT devices must be scalable to handle the volume of data generated. This requires a robust and reliable infrastructure that can handle the data generated by IoT devices.
- Maintenance: IoT devices require regular maintenance to ensure that they continue to function properly. In defence systems, this can be challenging because maintenance may require taking the system offline, which can disrupt operations.
- Physical security: IoT devices in defense settings may be vulnerable to physical attacks, such as theft or tampering. It is important to ensure that these devices are properly secured and monitored to prevent unauthorized access or interference [23-24].

Table 1
Advanced sensors features in defense use cases

Sensor Type	Functionality	Power Consumption	Accuracy	Applications
Acoustic	Detect and measure sound waves underwater or in air	Low to Moderate	High	Anti-Submarine Warfare (ASW) and Missile Detection
Hydrophones	Detect underwater sound waves	Low to Moderate	High	Submarines, Ships, Underwater platforms
Sonorous	Track undersea targets	Low	High	Anti-Submarine Warfare (ASW)
Acoustic Arrays	Identify sound waves in specific directions	Low to Moderate	High	Underwater object detection
Acoustic Cameras	Produce images using sound waves	Low to Moderate	High	Underwater imaging, Object detection
Optical Sensors	Detect and measure light or electromagnetic waves	Low to Moderate	High	Target Detection, Weapon Tracking and Situational Awareness.

Table 1 highlights the scope and utilization of vital sensors used in military applications. Feaures like types of sensors, functionalities, accuracy level and applications of these sensors are summarized.

7. Conclusion and Future Work

Modern military tactics are changing as Internet of Things (IoT) technology is being adopted more widely. Military organizations now have access to unprecedented levels of tactical awareness and operational effectiveness thanks to the Internet of Things (IoT), which enables the connection and real-time monitoring of a wide variety of devices and sensors. The ability to gather and evaluate data from various sources is one of the main advantages of IoT in military technology. Everything from cars to weapon systems can use sensors and devices to provide real-time data on position, performance, and upkeep requirements. Machine learning and artificial intelligence algorithms can be used to evaluate this data in order to produce predictive analytic and actionable insights that can assist armed groups in making better choices. IoT is giving military groups unprecedented levels of tactical awareness and operational effectiveness by enabling the connection and real-time monitoring of a wide variety of devices and sensors. The capacity to gather and evaluate data from a variety of sources is one of the main advantages of IoT in military technology. To provide real-time information on position, performance, and upkeep requirements, sensors and devices can be installed in everything from vehicles to weapon systems. This data can be examined using machine learning and artificial intelligence tools to produce predictive analytic and actionable insights that can assist armed groups in making better choices. In summation, the IoT is playing an increasingly important role in military activities and is quickly evolving in the field of defense technology. IoT is giving military companies a wealth of new powers and insights, from boosting situational awareness to increasing operational effectiveness. To guarantee the dependable and efficient functioning of these systems, it is crucial to handle the issues related to IoT in defense technology, such as security and environmental variables. IoT is likely to play an even bigger part in military technology in the years to come with ongoing innovation and investment, revolutionizing how militaries function and engage with the outside world.

Acknowledgements

<to be added>

References

[1] Mishra, S., Mahanty, C., Dash, S., & Mishra, B. K. (2019). Implementation of BFS-NB hybrid model in intrusion detection system. In Recent Developments in Machine Learning and Data Analytics: IC3 2018 (pp. 167-175). Springer Singapore.

[2] S. V, S. R, A. B, V. S. V and P. Vigneswari, "IoT based Healthcare Monitoring and Tracking System for Soldiers using ESP32," 2022 6th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2022, pp. 377-381, doi: 10.1109/ICCMC53470.2022.9754076.

[3] A. Utsav, A. Abhishek, P. Suraj and R. K. Badhai, "An IoT Based UAV Network For Military Applications," 2021 Sixth International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 2021, pp. 122-125, doi: 10.1109/WiSPNET51692.2021.9419470.

[4] Jena, L., Kamila, N. K., & Mishra, S. (2014). Privacy preserving distributed data mining with evolutionary computing. In Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2013 (pp. 259-267). Springer International Publishing.

[5] Das, M.L. (2015). Privacy and Security Challenges in Internet of Things. In: Natarajan, R., Barua, G., Patra, M.R. (eds) Distributed Computing and Internet Technology. ICDCIT 2015. Lecture Notes in Computer Science, vol 8956. Springer, Cham. https://doi.org/10.1007/978-3-319-14977-6_3

[6] A. Pant (2019): Internet of Things Centricity of Future Military Operations, Journal of Defence Studies, Vol. 13, No. 2, April-June 2019, pp. 25-58, available at : https://idsa.in/jds/jds-13-2-2019-future-military-operations.com

[7] Gotarane, Vishal & Raskar, Sandeep. (2019). IoT Practices in Military Applications. 891-894. doi: 10.1109/ICOEI.2019.8862559.

[8] J.-M. Martinez-Caro, M.-D. Cano, "IoT System Integrating Unmanned Aerial Vehicles and LoRa Technology: A Performance Evaluation Study", Wireless Communications and Mobile Computing, vol. 2019, Article ID 4307925, 12 pages, 2019. https://doi.org/10.1155/2019/4307925

[9] Joshi, Ninad & Joshi, Sumedh & Jojare, Malhar & Askhedkar, Anjali. (2021). IoT based Smart Vest and Helmet for Defence Sector. 1-8. doi: 10.1109/ICCICT50803.2021.9510067.

[10] Iyer, B., Patil, N. IoT enabled tracking and monitoring sensor for military applications. Int J Syst Assur Eng Manag 9, 1294–1301 (2018). https://doi.org/10.1007/s13198-018-0727-8

[11] Bognar, Eszter Katalin. (2018). Possibilities and security challenges of using IoT for military purposes.

[12] Joe Mariani, Brian Williams, Brett Loubert (2015). Continuing the march: The past, present, and future of the IoT in the military. available at: https://www2.deloitte.com/za/en/insights/focus/internet-of-things/iot-in-military-defense-industry.html

[13] J. J. Kang, W. Yang, G. Dermody, M. Ghasemian, S. Adibi and P. Haskell-Dowland, "No Soldiers Left Behind: An IoT-Based Low-Power Military Mobile Health System Design," in IEEE Access, vol. 8, pp. 201498-201515, 2020, doi: 10.1109/ACCESS.2020.3035812.

[14] Sehrish Mudassar. (2022). IOT BASED RESOURCE SCHEDULING FRAMEWORK FOR MILITARY. International Research Journal of Modernization in Engineering Technology and Science. Volume:04/Issue:02/February-2022. available at: https://www.irjmets.com/

[15] R. Abhishek, S. Caroline and A. D. Jose Raju, "IoT Driven Defence Vehicle System," 2019 International Conference on Recent Advances in Energy-efficient Computing and Communication (ICRAECC), Nagercoil, India, 2019, pp. 1-4, doi: 10.1109/ICRAECC43874.2019.8995073.

[16] M. Sabarimuthu, M. P. Krishna, P. M. Sundari, L. Aarthi, P. M. Juhair and G. GowthamRaj, "IoT Based Soldier Status Monitoring Using Sensors and SOS Switch," 2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA), Gunupur, India, 2022, pp. 1-6, doi: 10.1109/ICCSEA54677.2022.9936125.

[17] Singh, P., & Mishra, S. (2022). A Comprehensive Study of Security Aspects in Blockchain. In Predictive Data Security using AI: Insights and Issues of Blockchain, IoT, and DevOps (pp. 1-24). Singapore: Springer Nature Singapore.

[18] Sahoo, S., & Mishra, S. (2022, November). A Comparative Analysis of PGGAN with Other Data Augmentation Technique for Brain Tumor Classification. In 2022 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC) (pp. 1-7). IEEE.

[19] Ghosh, S., & Mishra, S. (2022, November). Intelligent Virtual Ambulance Model using Predictive Learning. In 2022 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC) (pp. 1-5). IEEE.

[20] Mishra, Y., Mishra, S., & Mallick, P. K. (2022). A Regression Approach Towards Climate Forecasting Analysis in India. In Cognitive Informatics and Soft Computing: Proceeding of CISC 2021 (pp. 457-465). Singapore: Springer Nature Singapore.

[21] Periwal, S., Swain, T., & Mishra, S. (2022). Integrated Machine Learning Models for Enhanced Security of Healthcare Data. In Augmented Intelligence in Healthcare: A Pragmatic and Integrated Analysis (pp. 355-369). Singapore: Springer Nature Singapore.

[22] Mishra, S., Tripathy, H. K., Kumar Thakkar, H., Garg, D., Kotecha, K., & Pandya, S. (2021). An explainable intelligence driven query prioritization using balanced decision tree approach for multi-level psychological disorders assessment. Frontiers in public health, 9, 795007.

[23] Mishra, S., Mishra, B. K., & Tripathy, H. K. (2015, December). A neuro-genetic model to predict hepatitis disease risk. In 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC) (pp. 1-3). IEEE.

[24] Chattopadhyay, A., Mishra, S., & González-Briones, A. (2021). Integration of machine learning and IoT in healthcare domain. Hybrid artificial intelligence and IoT in healthcare, 223-244.