RESEARCH & INNOVATION DIVISION
IJIST

The Emergence of the Internet of Things in Military Defense: A Comprehensive Review

Muhammad Kashif[1], Naila Latif[*2]
[1]Department of Information Technology, Government College University Faisalabad, Punjab, Pakistan.
[2]School of Telecommunication Engineering, Xidian University, Shaanxi, Xi'an, China.
[*]**Correspondence:** mkalvi94@hotmail.com, nailalatif93@gmail.com

Citation | Kashif. M, Latif. N, "The Emergence of the Internet of Things in Military Defense: A Comprehensive Review", IJIST, Vol. 06 Issue. 04 pp 2159-2179, Dec 2024
Received | Nov 24, 2024, **Revised |** Dec 16, 2024, **Accepted |** Dec 22, 2024, **Published |** Dec 24, 2024.

The Internet of Things (IoT) has emerged as a significant research field. The main concept of IoT technology is to connect millions of devices and facilitate interaction between these devices and the cloud. Recently this concept has been considered and applied in the design of systems intended for distributing data and information between heterogeneous devices. The goal is to enhance the performance of the business and decision-making process. IoT enables energy and supply chain monitoring, production coordination, equipment performance optimization, transportation, and public health, to improve, and enhance worker safety. It is revolutionizing military operations enhancing battlespace awareness operational efficiency, and command structures while enabling more intelligent and responsive security systems across diverse defense sectors and mission domains. This paper discusses how IoT technology shapes the future of military information and defense systems. The goal of this article is to present a comprehensive literature review on the application of IoT in military defense. This review also puts future recommendations for the further development of IoT technology in the defense sector.

Keywords: Internet of Things (IoT), Military Defense, IoT Security, Battlespace Awareness.

Introduction:

The evolution of the Internet of Things (IoT) has been marked by significant milestones and technological advancements over the years. The Massachusetts Institute of Technology initially defined the concept of the Internet of Things (IoT) in 1999. It was later introduced in 2005 through the International Telecommunication Union's IT Internet Report [1]. The Fourth Industrial Revolution further accelerated IoT's integration into daily life, and other technologies such as artificial intelligence and big data analytics enhanced its ability to improve human quality of life through effective data sharing and analysis [2] This integration represents a large wave in the information market, initiated by the advent of computers, mobile phones, and the world wide web. By 2020, approximately 14 billion IoT devices were interconnected worldwide, illustrating the fast development of this field [3]. This emergence demonstrates how technology advancements are driven by societal demand to form the current ecosystem of IoT applications and its challenges.

IoT on the other hand is an emerging technology that connects various devices to the Internet through identification, data acquisition, localization, tracking, and monitoring. Therefore, the interconnectivity has brought revolutionary changes in the world's political, economic, and even cultural aspects, making the IoT a famous debate. These changes have various consequences that affect dozens of domains, from simple interactions of consumers with manufactured products to widespread logistics and industries. For example, in the industrial sector, IoT improves performance in supply chain management as well as in maintaining appliances thus reducing costs and increasing productivity [4]. In healthcare, the IoT ensures drug and patient tracking since this leads to efficiency and increased operation safety [4]. Integrating IoT with data analytics enables industries to forecast the demands of their products and services to be able to prevent any interruption. Realizing how IoT can bring about change, several governments, firms, and military entities have sought its implementation. IoT provides great advantages in the military field primarily in the enhancement of warfare awareness and network warfare while posing security risks that have to be solved [5]. The use of IoT in defense applications has evolved considerably since early implementations of unattended sensors to monitor strategic movements during mid-20th-century wars [6]. With time, advancements in IoT allowed the integration of multi-domain capabilities, combining AI with real-time data exchange to support mission integration, secure communication, and enhanced situational awareness across diverse defense environments.

Building on these advancements, Many IoT propositions are useful for current military operations, including asset tracking in real-time, constant monitoring of troop health, and managing supplies [7]. There are also reviews of the integration of autonomous systems and robotics including drones and surveillance robots for reconnaissance as well as combating techniques which are safer since the risk posed to humans is concerned. The concept of cybersecurity is presented as one of the main risks and challenges of implementing this technological concept [7]. As military forces continue to rely on information flows, closely-knit operations and cooperation within the coalition such as NATO, and IP and the security of these IoT systems will be of the essence as far as dominance and cooperation are concerned [8]. Consequently, the future of warfare is set to be fixed at the intersection of technological features and elaborate international relations.

Relevance to Military Defense:

In the context of military defense, IoT incorporates a wide range of components, including soldiers, military vehicles, ships, tanks, aircraft, satellites, and unmanned aerial vehicles (UAVs) [9]. These interconnected elements form a comprehensive ecosystem that enhances situational awareness and creates a more responsive defense infrastructure. Our comprehensive review explores the integration of IoT in military applications, examining its potential to

revolutionize defense operations, enhance situational awareness, and improve overall military effectiveness [10]. The rapid advancement of technology, including cloud computing, mobile communication, sensor networks, and artificial intelligence, has created both challenges and opportunities for military defense and national security. The Internet of Things presents transformative potential for military applications offering unprecedented capabilities to enhance operational tempo adaptability and effectiveness across defense systems and platforms. The adoption of IoT technologies in military defense is essential due to several key factors:

- Enhanced Situational Awareness: IoT enables the constant monitoring, control, and acquisition of environmental status, human and vehicular traffic, and the status of the equipment that would be necessary for immediate response during emergencies [11].
- Improved Operational Efficiency: The integration of IoT increases overall communication, coordination, time, resource management, and logistics in military operations so overall better strategies can be executed [12].
- Advanced Surveillance and Reconnaissance: UAVs, sensors, and cameras powered by IoT help to enhance surveillance and reconnaissance functions improving the intelligence support for military decisions [10].
- Soldier Enhancement: The soldier-wearable IoT devices improve performance, safety, and health on the battlefield and could save lives and improve the rate of success in combat missions.
- Training and Simulation: IoT integrated with virtual and augmented reality offers a state-of-the-art training environment for the military in various complex situations.

The remainder of this paper is organized as follows. Section 2 presents the methodology, which is used for the literature review. Section 3 presents some promising key insights into the utilization of IoT technologies in defense applications. Section 4 introduces the integration of IoT in military systems. Section 5 reviews the basics of the IoT and Artificial Intelligence for tactical and emergency environments. Section 6 describes the main shortcomings, and outlines the current challenges. Section 7 identifies further research areas in the future. Finally, Section 8 is devoted to conclusions.

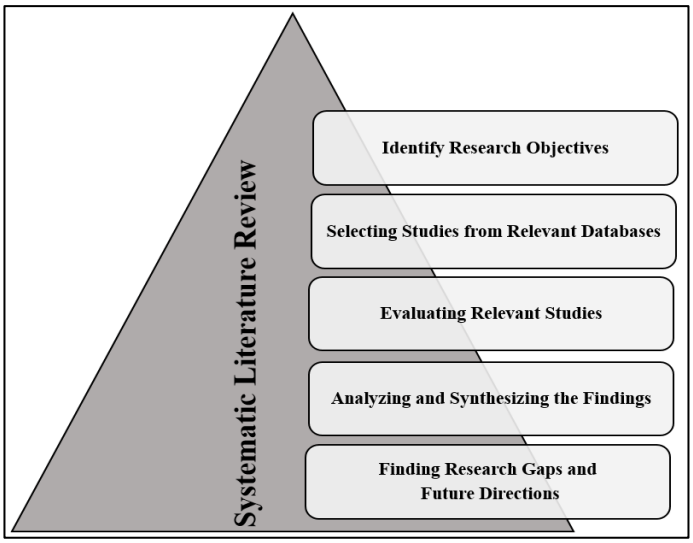

Figure 1. The figure explains the systematic flow of literature.

Methodology:

This review will help users and researchers understand and appreciate the place of IoT technologies in military defense. A systematic approach was used to determine relevant literature in the field and to select and analyze it appropriately. Figure 1 illustrates the systematic flow of literature.

Objectives of the Study:

The integration of IoT in military defense represents a significant leap forward in technological capabilities, offering the potential to create more intelligent, autonomous, and effective defense systems. The key contributions of this study are:

- To systematically review IoT technologies and existing challenges in military defense and explore future possibilities for their advancements.
- To examine the role of IoT in improving operational effectiveness, optimizing resource utilization, and improving topographical awareness in military operations.
- To explore how IoT devices helped to enhance surveillance and reconnaissance efforts.
- To evaluate how IoT technologies can be leveraged to enhance soldier performance, safety, and health during military operations.
- To identify the security and privacy challenges associated with the implementation of IoT in military defense and propose valuable solutions to mitigate these issues.

Data Collection:

Literature research was conducted in several academic databases such as IEEE Explore, Springer, and Science Direct. In the search process, the authors aimed to find articles published in the last five years and more specifically, those discussing the integration of IoT in defense systems.

Key Search Strings:

These search terms were employed to find the relevant literature; "military IoT," "Defense IoT technology," "military IoT systems," and "IoT in "IoT in command and control

Inclusion Criteria:

The primary focus was on peer-reviewed journal articles, conference proceedings, white papers, and government reports that discussed:

- IoT technologies applied in military systems.
- Security, communication, and logistical challenges related to IoT in defense.
- Innovations in IoT for enhancing situational awareness and operational efficiency in military contexts.
- Additionally, studies that provided empirical evidence or case studies on real-world applications of IoT in defense were prioritized.

Organization and Analysis:

The collected literature was grouped into categories and subcategories based on IoT architecture, sensor technology, cloud and fog computing, and their uses in military operations such as surveillance, logistics, and warfare. Each theme was further analyzed to highlight trends, challenges, and advancements in IoT technologies. Comparative analysis was also employed, particularly for studies that presented different approaches to utilizing IoT in various military domains, including command and control systems and surveillance technologies.

Key Insights into the Utilization of IoT Technologies in Defense Applications:

IoT Architecture and Components:

The IoT architecture in military defense involves interconnected physical objects embedded with sensors and processing capabilities, exchanging real-time data over public and military networks [13]. This interconnected ecosystem includes combat gear with biometric wearables, sensors for various data collection, smart guns, and more, enhancing the military collection [13]. To address the security challenges in this heterogeneous environment, a Blockchain-empowered auditable platform is proposed for the Internet-of-Battlefield Things (IoBT), ensuring trust and privacy in information exchange among battlefield entities [8][14]. Collaborative efforts between human operators and advanced AI systems are increasingly crucial

for navigating the complex cyber domain, enabling stronger defense strategies and enhancing national cybersecurity.

Sensors:

Sensors are persistent devices designed to obtain and transmit data on different positions, conditions, and appliances [15]. For example, Light-dependent Resistor (LDR) detects the light and sends the output to the circuits. Similarly, recent innovations in sensor technology include various state-of-the-art advancements of IoT for military applications involving a range of cutting-edge developments. Such as Additive manufacturing (AM) has turned out to be an advance technique in sensor technology that is used to design and develop high-performance 3D-printed sensors for tracking soldiers in a war zone [16]. At the same time, there is a major concern about building IoT-based sensing devices, which will facilitate the real-time monitoring and tracking features in the battlefields through the IoT capabilities of sensors. Conversely, in the pathophysiological and biochemical aspects of trauma, continuous progress and development have made devices such as near-infrared spectrometry (NIRS) and portable thromboelastographic (TEG) in small size.

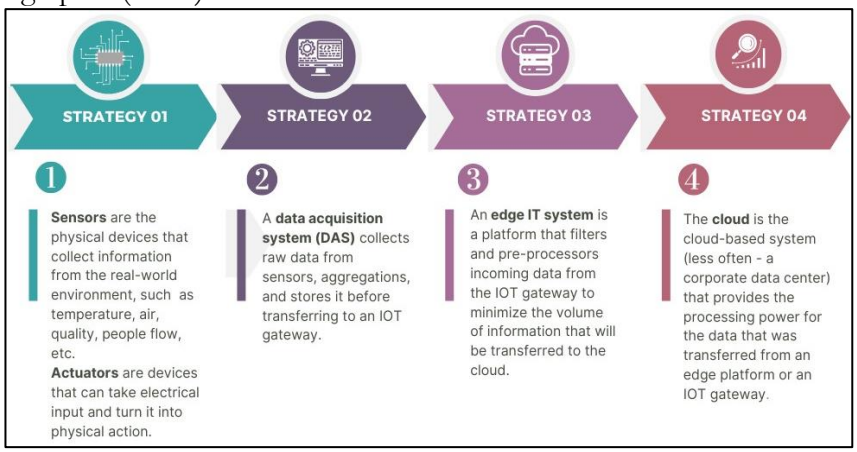

Figure 2. The figure explains the stages of IoT architecture.

They facilitate constant monitoring of the physiological condition and data acquisition, to improve healthcare services in the challenging environment of a war zone [16]. Overall, these advancements highlight the essential role of sensor technology in improving soldier safety, performance, and mission effectiveness.

Framework Gateway:

The IoT framework gateway serves as the intermediary between device nodes and the external internet, facilitating data collection and transmission. These gateways enable real-time interconnectivity of related devices and enable real-time data exchange making efficient warfare strategies a reality such as secure communication and decision-making capabilities [16]. When edge intelligence is applied to IoT wearables, the functions of these devices could be enhanced to perform operations such as estimation of directions in gunshots thereby increasing efficiency. In military applications, security is paramount and therefore it becomes essential to design and implement robust security measures in hardware, network, and application layers to protect data from attack. The use of technologies like Software-Defined Networking (SDN) and Distributed Ledger Technology (DLT) helps to build the elements of decentralized, energy-saving, and secure communication systems necessary for successful military operations in today's complex and dynamic environments [17].

Cloud:

Servers of IoT systems that are built for the military defense, are deployed in cloud environments in order to gather and categorize information, and then critically analyze this information. These are open-source platforms, offering basic functionalities for the server side

of the IoT architectural structure allowing for proper connectivity of devices employed in military activities. Information that is transmitted through the cloud is compiled and kept with great confidentiality so that the right decisions are made and immediate actions are taken on the field. The reliability of military servers is a crucial factor in the use of applications.

When a server has a problem, then resources in the cloud are reallocated to maintain system availability which is important during defense activities. There are solutions such as the WSO2 IoT server [18] that provide integrated solutions to military organizations on how to handle the connected devices and create secure applications as well as protect confidential information. Also, these servers provide support for enterprise mobility management, which means they solve issues related to mobile computing that are crucial for modern military tactics.

Mobile/User Applications:

IoT defense system has mobile and user applications as one of the paramount layers that improve communication, monitoring, and control. These applications are essentially meant to link military individuals as well as equipment in a direct manner so that there could be an appropriate exchange as well as processing of data. For instance, a metal detector robot that is in collaboration with ZigBee which is a device that is predominantly used in the IoT systems is operated by a mobile application. Admin communicates this to the robot through a mobile application forward, backward left, or right receiver performs the task when instructed. Some of the benefits received from IoT implementation in the defense sphere include object tracking, health monitoring, drone surveillance, and others leading to an increase in situational awareness and operational effectiveness [19][20]. The war in the future will consist of devices connected to the internet containing sensors and the capacity to process information and cooperate through IoT. This means there is a need for profound security and analytics. This is an integration of IoT and network-centric warfare, which offers a new architectural blueprint referred to as IoT Net War that uses sensors and gateways together with the internet and cloud services that redefine military operations.

Key IoT Technologies Used in Defense:

RFID Technology and the Internet of Things:

Another advancement in IoT systems is the utilization of RFID (Radio Frequency Identification), which represents the primary mechanical recognition of the IoT. RFID technology is employed to track and monitor products wherever needed, particularly within the supply chain segment [21]. The frequency range for RFID spans from 125 kHz to 5.8 GHz, and RFID tags consist of at least three basic components. The integrated circuit (IC) collects and monitors all information related to the input and output of products. IoT sensors transmit information wirelessly to receiving devices enabling real-time monitoring and analysis of environmental conditions or equipment status. The transmitter device is responsible for transmitting information in the form of signals to the sender and receiver. The packaging covers the chip and transmitter, enabling the attachment of tags to objects for identification. Various industries, particularly logistics, are adopting RFID to improve their tracking and monitoring processes.

In addition to RFID, several other innovative technologies are used to track and identify objects. For instance, one-dimensional barcodes (ID) have made significant contributions to supply chain management and various industries, including asset management and defense projects. Two-dimensional (2D) barcodes, while providing a richer source of data, are not updatable once printed. In contrast, RFID stands out due to its exceptional ability to support automated data capture (ADC) procedures by collecting and processing environmental data, making it a key technology for goods identification in military contexts.

The latest trends in RFID technology, including IoT are set to revolutionize military defense systems in 2023 and 2024. This integration increases possibilities like real-time object

tracking, healthcare monitoring, and drone surveillance, all of which dramatically increase situational and resource management. The concept of the Internet of Battlefield Things (IoBT) also opens up new opportunities to improve the network Quality of Service (QoS) through user access control and performance optimization and solves the main issues such as cyberattacks and resource management. The adoption of IoT solutions in air and missile defense systems not only strengthens subsystems but also enhances overall system capabilities, demonstrating the potential for improved performance and streamlined procedures in military operations [19][22]. These advancements signify a significant shift towards more secure, efficient, and robust defense systems, illustrating the critical role of RFID technology in modern military applications.

IPV6(Internet Protocol version 6):

IPv6 is the new addressing system for internet services and devices, designed to accommodate the growing number of internet users worldwide. As the demand for internet addresses increases, IPv6, also known as the Internet Protocol Next Generation, has become essential. The Internet Engineering Task Force (IETF) has developed and studied this latest version to replace IPv4, ensuring sufficient addresses for billions of connected devices in the future [23]. IPv6 is particularly beneficial for IoT devices, ensuring better performance across various applications. The advantages of IPv6 include automatic configuration when any device connects to services, eliminating the need for manual subnetting. It also enhances multicast routing, offers flexibility for extensions, supports predefined authentication and privacy, and provides proper quality of service.

Cloud Computing:

The relationship between cloud computing and IoT is a fundamental key in emerging technologies, particularly in military applications where data-driven decision-making is important. Both technologies collaborate to advance new trends in Information and Communication Technologies (ICT), enhancing capabilities in military operations such as real-time surveillance and intelligence gathering [24]. IoT produces a massive number of data arising from devices like drones and sensors; cloud computing ensures that such data is safely stored, retrieved, and transmitted via different communication technologies, thus making information on the battlefield easily available [25]. This process is achieved without relying on physical infrastructure on physical infrastructure, or software, thereby increasing the speed and efficiency of operations in dynamic combat environments.

The cost of cloud computing is significantly lower compared to physical devices, allowing military organizations to allocate budgets more effectively towards critical services such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Cloud computing allows military personnel to access data anytime and anywhere via the Internet, which is essential for effective field operations and strategic planning. IoT devices, such as battlefield sensors, directly connect to cloud services, where generated outputs are processed and stored for real-time analysis and operational coordination. Advancements in cloud computing technology within military defense systems are expected to focus on enhancing security through frameworks like AWS and flexible resource allocation strategies to adapt to mission demands [26]. The integration of AWS technology with cryptographic techniques will ensure secure communication within defense teams, which is vital for maintaining operational integrity during combat scenarios [27]. Load-balancing algorithms will play a critical role in distributing computing resources based on operational priorities, ensuring that mission-critical tasks receive the necessary computational power for timely execution. Virtual computing and defense technologies integrated into cloud infrastructures bolster network resilience by implementing robust authentication protocols and securing virtual machine environments crucial for protecting classified military activities and sensitive operational data. Advancements in cloud computing tools will address issues of consistency, fault tolerance, and security, enabling

the creation of high-assurance applications key for military strategies, while also reducing vendor lock-in to maintain flexibility in defense operations. This capability will allow the military to leverage cloud resources effectively, aligning with the growing demands for defense and security applications while emphasizing robust data protection and system sustainability within modern data centers, ultimately enhancing mission success. Significant advantages of cloud computing for military defense include improved scalability, cost efficiency, and operational effectiveness.

Table 1. Differences between IPv4 and IPv6 in security protocols and addressing schemes.

Feature	IPv4	IPv6
Addressing Scheme	A 32-bit address, it can address about 4.3 billion unique nodes.	128-bit address, compatible with up to 340 undecillionth unique addresses, with the capability of accommodating various devices.
Address Format	Dotted decimal format (e.g., 192.168.0.1).	Hexadecimal format, divided by colons (e.g.,2001:0db8:85a3:0000:0000:8a2e:0370:7334).
Address Exhaustion	Restricted number of addresses making them exhausted at some point.	Huge address space removes the issues tied to address exhaustion.
Security Protocols	Optional; IPSec is an optional protocol and is not mandatory.	IPSec is mandatory since it supports built-in and end-to-end encryption and authentication mechanisms.
NAT	Because of address shortage, it is widely used however, it adds complexity to security.	Not required because of a large number of addresses that help to make the network configuration and protection easier.
Auto-Configuration	Requires manual or DHCP-based configuration	Stateless address auto-configuration is supported, which enhances network size control and protection.

The above comparative table provides the comparison between IPv4 and IPv6 and highlights significant differences in addressing schemes and security protocols.

For instance, cloud computing enables the deployment of distributed systems at the edge of networks lowering latency and enhancing security in tactical domains. But these are revealed with some constraints, especially with the issue of security. In their application of cloud services, the military experiences threats such as data leakage, account fraud, and below-par adherence to security requirements [1]. To manage these risks, a strong risk management system is required that integrates constant auditing and third-party verification to foster user confidence [1]. Replacing traditional systems with cloud-based solutions introduces critical security challenges that must be addressed to ensure the safeguarding of sensitive military data [28]. Cloud computing has brought about revolutionary opportunities for military operations; nevertheless, those opportunities should be understood and analyzed properly to avoid facing the main difficult issues.

Fog Computing:

Fog computing, often referred to as edge computing, represents an innovation in cloud computing, developed in response to the widespread adoption of cloud technologies across various sectors. Many IoT devices lack the computational power needed for independent data processing, and fog computing addresses this limitation by enabling data reception and processing closer to the source from low-power devices [29]. This technology facilitates collaboration among research agencies, sensors, and connected machines, allowing for immediate analysis through nearby edge devices, such as switches. Recent advancements in fog computing technology are particularly relevant for military defense systems. For instance, fog computation models are being developed to access military vehicles from connected garages

secured through blockchain networks, ensuring secure and immediate decision-making capabilities while reducing operational costs. These capabilities are crucial for military operations that depend on the timely collection, transmission, and analysis of critical information. Fog-based systems contribute to efficient damage assessment and recovery algorithms that reduce downtime after attacks and improve data integrity and security in military applications [30].

Another innovative application involves the integration of fog computing with brain-computer interfaces (BCI), enabling real-time monitoring and analysis of EEG brain waves. This opens new possibilities for physiological action observation and machine communication in military settings, improving situational awareness and operational effectiveness. Fog computing notably improves capabilities to collect and process data at the network's edge a crucial aspect of current warfare. Thus, optimizing overall latency and the use of bandwidth contributes to faster analysis of data coming from numerous sensors installed at the scene to respond to threats [29]. In addition, it has a hierarchical structure, enabling local data processing, which is crucial for preserving operational security and preventing data leakage. Military operations face ongoing security risks including potential vulnerabilities to sniffer attacks and jamming devices, which could compromise mission effectiveness and troop safety [31]. To mitigate these threats, there is needed proper protection measures like encryption and intrusion need to be implemented to protect vital information [31]. There are issues of managing a large number of devices participating in fog computing, which requires effective algorithms and protocols for cooperation between them. Fog computing improves the overall efficiency in the operation of military defense systems; work still needs to be done for security threats to be handled efficiently [32]. Its effectiveness, therefore, will lie in the ability to strike an appropriate balance between the new approach it brings and the necessary security controls that meet emerging threats.

Integration of IoT in Military Systems:

Examples and Case Studies of IoT Applications in Military Defense:

Implementing IoT in military systems can significantly enhance and improve the mechanism of defense capabilities. The 21st century has introduced the concept of connected battlefields through advanced technologies. Numerous countries have tasked their research and development agencies with transforming military defense systems to prepare for the next generation of connected battlefields. Leading defense research organizations globally are investing in IoT-enabled technologies to advance situational awareness, communication security, and strategic data analysis capabilities on the battlefield. These advancements include the development of sophisticated sensors, radars, and AI-driven systems to support real-time data collection, threat detection, and secure information exchange. The continued evolution of IoT in defense aims to enhance security measures, provide tactical advantages, and bolster overall resilience in complex combat environments [33][34].

Military IoT devices can identify various threats, including artillery guns and firearms, explosives, armed forces, snipers, and more. The IoT concept in the military collects data from individuals, equipment, and materials using sensors and shares this information among military units, monitoring systems, and control centers through a communication infrastructure. Military defense systems are advancing with the integration of IoT technologies, creating interconnected networks known as the Internet of Battle Things (IoBT) [35]. These systems use sensors, wearables, unmanned aerial vehicles (UAVs), and other equipment embedded with biometric wearables and various sensors for data collection. To ensure security and agility in these IoT ecosystems, a multi-layer defense-in-depth cybersecurity mechanism is being implemented at the hardware, network, and application levels, utilizing Software Defined Networking (SDN) and technologies like Information-Centric Networks (ICN) and Delay-Tolerant Networks (DTN) [33]. Advancements feature smart systems like vests and helmets embedded with sensors,

modules, and cutting-edge wireless communication technology designed to improve functionality and safety for military personnel.

Applications of IoT in the Military:

Military activities during the war and professional exercises are much more critical these days. Many countries have adopted high-tech scientific abilities for defense and our enemies, which is why advancement in defense via new technologies is very important. The research and development agencies take action in progressively under-pressure atmospheres and controlled situations. The Internet of Things (IoT) is a possible solution to this issue [36]. Considering the current military foundations, we have laid out three separate areas for IoT military applications.

Data Warfare:

By gathering information from a wide range of military platforms, including fighter jets, weapons, and formations of soldiers, the military can enhance the effectiveness of their intelligence and surveillance systems. This wealth of data will enable the military to identify key threats more quickly and accurately. Using IoT technology and unmanned aerial vehicles (UAVs) in combat scenarios will be a key strategy on the battlefield, focusing on maintaining IoT connectivity and optimizing strategies for both attackers and defenders. This integration of IoT technology with Data Warfare will enhance predictive battlefield analytics, security strategies, and overall operational efficiency, revolutionizing military operations and decision-making processes in the coming years.

Table 2. Overview of IoT Applications in Data Warfare

IoT Application	Functionality	Real-World Example	Impact on Data Warfare
Drone Based Surveillance	Real-time monitoring, video/ thermal data acquisition.	Use of UAVs in Afghanistan/Iraq for tracking insurgents and monitoring enemy movements	Employment of UAVs in conflicted zones for identification of rebels and of movements of the opposite party.
Cyber Warfare	Cybersecurity, networking, data gathering, and attackers' activities	The WannaCry Ransomware attack in May 2017 exploited IoT vulnerabilities in military networks.	Reveals vulnerabilities of interconnected devices, and increases the significance of cyber security and actions protection strategies.
Battlefield Sensors	Surveillance of the environment, troops, and their equipment	The JADC2 system of the U.S. Army manages sensors for multi-domain command & control.	Enhances the real-time data collection from diverse sources, improving decision-making and response times during combat.

The table highlights the revolutionary impact of IoT technologies across different aspects of data warfare.

Smart Bases:

Including IoT devices in military headquarters has various positive impacts, such as while building smart bases automated security screening enhances safety while reducing the need for labor. Digital cameras equipped with high-tech technology are connected by a controlled and secure subnetwork, increasing security. Smart observational devices track all types of movement to improve performance. These subsystems are integrated into a central administrative system, which helps to reduce security risks. Connected to the internet to offset risks within any tenable physical status. The smart bases are equipped with intelligent devices to manage all resources

and boost the performance of the base. Such as biometric wearables, sensors for several purposes, smart guns, and other military equipment will be common, making military assets more efficient. In the future, this ecosystem will be needed for predictive battlefield analytics, security measures, and a decentralized IoT network architecture. The integration of efficient private blockchain systems like Hyperledger Fabric will enable end-to-end security, mobility, and bi-directional communication, enhancing Smart Base technology in military defense systems [36].

Applications in Logistics:

The Internet of Things (IoT) has significantly influenced logistics and inventory systems, benefiting sectors such as agriculture and healthcare. The military's logistics department, responsible for moving assets and equipment, can also leverage IoT applications. Developed countries are already utilizing IoT systems and observational devices for advanced logistics management. RFID technology, in particular, enhances supply management by providing comprehensive tracking from the source to the destination.

Fire Control Systems:

Fire control technology within IoT; advanced deep learning models-based systems will monitor and detect fires in forests, apartments, and industrial buildings in real-time and be continuously alarming. The development of a large-scale Flame and Smoke Detection Dataset (FASDD) will accelerate the ongoing advancement of fire detection models. This will enable the training of deep learning algorithms to improve performance in recognizing and monitoring fires, with applications in collaborative fire observation and detection using satellites, drones, and ground sensors in an integrated network environment. These advancements signify a promising future for enhancing fire control capabilities through IoT technology in military defense systems.

Health Monitoring:

Specialized helmets equipped with control sensors are utilized to detect brain traumas, including concussions [36]. In combat situations, small yet sophisticated health monitoring and healthcare devices with intelligent telemetric capabilities are being used more frequently. This allows initial healthcare and first aid services to be provided to soldiers without requiring onsite personnel. One advanced system that has been deployed by the US, British, and Norwegian armies is the Tempus Pro, which can monitor virtual signals to help keep soldiers healthy and safe [37]. In the healthcare domain, IoT-enabled systems utilize sensors like heartbeat sensors, EKGs, and blood pressure sensors to collect vital signs, making healthcare more accessible and cost-effective for the general public. Similarly, in military defense systems, compact medical monitoring systems incorporating biosensors, Peltier crystals, and GPS technology are being deployed to monitor soldiers' health status, track their locations, and ensure their safety in challenging environments.

Advancements in IoT for Enhanced C4ISR Systems in Military Operations:

IoT technology offers significant advantages for Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance systems (C4ISR), which rely on extensive sensor networks across diverse platforms [38]. These networks encompass sensors deployed in unmanned aerial vehicles, radars, video cameras, infrared and passive infrared sensors, unattended ground sensors, and portable devices. They provide real-time data for combat troops and decision-makers, facilitating the creation of a unified operational picture that enhances coordination and control within operational areas. Efficient energy management is critical in combat scenarios to prolong device lifespan and conserve energy. Accordingly, hardware, communication protocols, and software elements are continually developed to optimize energy utilization [39]. Designing and operating military devices necessitates devotion to military equipment architecture and reliable transfer capabilities. Tactical networks ensure

encrypted communication and secure data transfer, albeit at slower rates compared to cellular networks. Efforts are ongoing in research projects focusing on wideband radio frequency solutions to meet IoT requirements. In [40] a next-generation radio system capable of supporting over 200 users simultaneously, enabling rapid data transfer while meeting stringent military encryption standards. Nevertheless, the processing of large volumes and diverse types of data remains a significant challenge. The integration of intelligence networks into combat operations began with specialized military programs that introduced advanced, Android-based devices designed for operational use. These devices, resembling commercial smartphones but tailored for military applications, include features like Blue Force Tracking, 3D maps, and targeting applications to enhance situational awareness on the battlefield. Data integration platforms consolidate and analyze information from multiple sensors across various platforms, offering comprehensive insights into the positions and movements of friendly and hostile forces, thereby improving coordination and control in combat environments.

Cooperative and Distributed Sensing:

Cooperative sensing in IoT offers advantages for managing mission scenarios without overwhelming sensors and their platforms with excessive equipment. Multiple devices can enter an area of interest and share sensing data to accommodate new or unforeseen requirements. For example, soldiers can enhance their situational awareness by leveraging cooperative sensing, thereby increasing mission success. Resource-rich devices can aggregate data from diverse sources to create a Common Operating Picture (COP), facilitating faster response times, informed decision-making, and reduced reliance on backhaul communications. Distributed sensing applications typically involve two primary components: deploying sensing devices and directly collecting resultant data from these devices. These applications pose several challenges that require mitigation. Serving a large user base while offering meaningful incentives presents a primary challenge. Ensuring data quality and security is also critical, given the potential for compromised devices to undermine overall system integrity, especially in environments adopting the" Bring your Device" (BYOD) paradigm [41][20]. Maintaining data accuracy in crowdsensing environments varies by domain and is complicated by the diverse capabilities and performance fluctuations of individual devices. Such as low battery levels in smartphones may lead to infrequent GPS updates, affecting geo-tagging accuracy. Techniques to ensure data reliability often involve over-sampling, anomaly detection, reputation systems for trustworthy sensing in public safety contexts, or human oversight through trust networks. Nevertheless, privacy risks persist in crowdsensing services, as geotagging and metadata can compromise user anonymity and reveal sensitive information about device activities.

Energy Management:

The US Department of Defense (DoD) is currently implementing energy efficiency projects in its facilities to reduce its energy consumption [42]. The use of data and predictive algorithms can also assist in understanding energy usage patterns more effectively and can lead to significant cost reductions for the military [43].

Artificial Intelligence (AI) and Internet of Things (IoT):

AI and IoT are increasingly recognized as complementary technologies gaining widespread adoption. Integration of AI is deemed essential for maximizing the practical utility of IoT, especially as networks expand in complexity and device numbers grow. AI plays a crucial role in processing, categorizing, integrating, and analyzing the vast volumes of heterogeneous data generated by diverse IoT devices and sensors, supporting a multitude of applications [44]. For instance, current estimates indicate that IoT generates over 2.5 quintillion bytes of data daily, facilitated by approximately 9 billion connected devices, equivalent to the storage capacity of 57.5 billion 32GB iPads per day. Artificial intelligence extends beyond human capabilities by providing multidimensional trend analysis within big data environments. AI systems excel in

dynamically regulating device operations by selecting appropriate devices, analyzing their outputs, adjusting operations to match conditions, coordinating actions with other devices, and optimizing outputs to environmental and network constraints. Such tasks are challenging to manage efficiently within large-scale database systems. IoT analytics heavily leverages deep learning techniques due to the sparsity and temporal nature of machine-generated data. These techniques mitigate challenges associated with data preprocessing and training algorithms, allowing continuous monitoring of sensor data in a cost-effective manner. Deep learning algorithms autonomously acquire new insights, thereby freeing developers to focus on strategic tasks rather than routine training processes [45]. The concept of "Ambient Intelligence" emerging at the intersection of AI and IoT, presents an intriguing development. Anticipated within the next decade or two, Ambient Intelligence envisions an enriched electronic environment where interconnected devices collaborate seamlessly to assist individuals in daily activities, tasks, and rituals. This environment harnesses hidden data and intelligence embedded within networked devices, emphasizing pervasive computing, contextual awareness, profiling, and human-centered interface design as defining features [46]. Security and protection of IoT activities and interconnected devices represent critical components within the domain. An essential aspect involves safeguarding against malicious infiltrations and cyberattacks that deploy malicious software codes to disrupt operations or cause erroneous execution. A notable instance of such an attack occurred with the Stuxnet worm in 2009, built by the USA and Israel entities, which targeted the Iranian nuclear program aimed at destroying critical infrastructure [47].

Further incidences like the DDoS attack on the French telecom provider OVH in September 2016 which affected telecommunications services, and the security threats that led to the removal of 500,000 pacemakers in August 2017 demonstrate that cyber threat is an adaptable and serious danger [37]. These threats can target different devices and last from a few seconds or minutes to days or even hours, thus in the case of IOT-enabled high-value networks and systems they can have broader disruption in case of a cyber-attack.

Even if IoT operations are conducted on separate networks, strong security measures are still necessary and integral because of external devices such as flash drives as it was shown in the Stuxnet case. Data security risks in IoT networks including industrial spying, monitoring, and unauthorized data collection, are inherent to the cybersecurity challenges. Therefore, protecting IoT requires strong solutions, such as segmented networks, malware detection, and removal tools, multi-level data encryption, regular firmware updates, and the use of blockchain technology. Blockchain, particularly, offers promising collaborations with IoT by providing encrypted, decentralized data storage solutions that enhance data integrity and security.

In military use cases, both Artificial Intelligence (AI) and Internet of Things (IoT) technologies have important roles in enhancing defense capabilities. Artificial Intelligence (AI) empowered with Machine learning algorithms, enables to process and analyze the patterns and anomalies detected from IoT networks, which is important for military operations. This interconnection of AI and IoT has led to Artificial Intelligence-of-Things (AIoT) systems, which are enhancing defense strategies by autonomous decision-making and proactive responses to dynamic operational environments [48]. Integration of AI with IoT triggers major security issues and the need to develop security frameworks to effectively address emerging risks.

Current Challenges and Limitations:

The Internet of Things (IoT) is the latest invention in the field of research. There are some challenges when we will implement this technology in any field of our life. The challenges are:

Standardization:

The research organizations have yet to design an identical standard format for an explanation of data information created by IoT devices to permit the collection of data coming

from different domains and providers [49]. For example, defense organizations of different countries are developing common interoperable communication architectures that facilitate efficient information flow across various branches. The primary purpose is to establish standardized frameworks to enhance coordination, streamline data exchange, and support seamless multi-domain operations [36].

Ethical Significance:

The ethical significance will be complex in the future for Internet devices [50]. For instance, the launching of unmanned aerial vehicles that incorporate IoT considerations into the battlefield brings a couple of ethical issues into the limelight. An example of the unauthorized deployment of drones was discussed in [36] and highlights the need for ethical policies concerning automation in decision-making, particularly regarding civilian safety and accountability.

Costs:

The cost of IoT equipment is much more expensive as compared to other devices. The implementation structure, design, sensors, tracking devices, and supporting material costs are also expensive [13]. In the future, when consumption usability will grow in different areas then the cost of these things is reasonable for everyone [51]. However, such defense organizations that have implemented IoT for analytical purposes to anticipate the need for equipment maintenance have been determined to benefit from such investments in both efficiency and cost-cutting in the long run. Real-life examples pointed above show how IoT can make sense financially by improving processes of maintenance and readiness [52].

Privacy and Security:

IoT devices collect extensive data, posing privacy and security challenges [53]. Military networks are advancing encryption protocols and access control measures to secure sensitive data during operations. Observations from the recent field exercises demonstrate that signal encryption technology plays a crucial role in preventing the leakage of sensitive details in high-risk operations involving defense-related IoT systems that need to protect the data integrity of the network [54].

Interoperability:

Achieving interoperability among various military IoT systems is crucial. For example, NATO's Allied Command Transformation has focused on developing interoperability standards that enable seamless communication between allied forces' IoT systems [55]. A notable case study involves joint training exercises where multiple nations successfully integrated their IoT capabilities to enhance situational awareness and collaborative decision-making.

Data Management and Curation:

The rapid growth of data generated by military IoT systems necessitates effective management strategies. This operational approach illustrates the importance of filtering and curating data to enhance situational awareness while minimizing cognitive overload for soldiers. Future military applications are limited by the availability of network resources, and they have to give preference to the most critical function, namely situation awareness, compared to many other functions realized by military applications. Hence, it is crucial to emphasize the aforementioned information for its further application in military operations.

Data Analysis:

The challenges of analyzing large datasets in military applications are significant. An important application of such technologies is the implementation of combat operations on edge technologies that allow the processing of data at source in order to boost tactical time and perform critical decision-making in concentric conditions. This capability enabled quick decision-making based on real-time data from battlefield sensors, demonstrating the necessity of localized data analysis to respond effectively to threats.

Future Directions:

Next-Generation Military IoT:

In future military operations, it is expected that IoT technology will be incorporated across large and interconnected scales involving multiple military networks. Globalization and other dynamics are changing the nature of warfare as a contemporary and future conflict, which requires battles to integrate technical platforms. Space-based assets are becoming crucial for communication and imaging, making them essential elements of the battlespace and likely targets for adversarial actions. The evolution towards multi-domain warfare is a prominent topic in recent literature, emphasizing simultaneous engagement across diverse domains. According to the Training and Doctrine Command, the multi-domain battle framework encompasses traditional domains alongside space, cyberspace, the electromagnetic spectrum, and the information environment [56].

Military IoT systems build upon civilian IoT principles while incorporating distinct software, device configurations, and frequency allocations. These systems leverage cloud computing, edge computing, fog computing, pervasive computing, and contextual search capabilities. They operate on segregated networks, with sensitive networks often isolated to enhance security. Robust software and encryption protocols akin to those used in secure banking servers are essential to safeguard data and communication integrity in military IoT deployments. Modern defense organizations around the world are integrating IoT systems into their army for effective human resource management and to enhance auto functionalities. They enable the transition to a more technical form of warfare that minimizes supply demands but increases efficiency on the battlefield. Strategic defense initiatives now include multi-layered missile defense systems integrating sensor, radar, and satellite data for cohesive defense operations [22].

Networking and computerization are pivotal for integrating forces within the battlespace, with networking infrastructure serving as a cornerstone. Achieving interoperability hinges on standardizing networking protocols and hardware data sharing across systems. Network-centric warfare (NCW) is a key idea of the modern military. The networking environment is critical within future integrated operations.

Unmanned ground vehicles, drones, tanks, artillery, ships, etc., and supportive systems such as radars and lasers are expected to dominate wars in the future. These will be largely autonomous systems that are expected to work in coordination with other systems to perform specific operations; this means that there must be a solid IoT platform that will enable the various systems to coordinate their activities well. In future conflicts, data transfer between entities in battlespace generates a huge volume of data network load that cannot be managed by human interference. Therefore, the application of automated asset control will be unavoidable in achieving the best results for operational activities.

Military Operations Other than War (MOOTW):

Military Operations Other than War (MOOTW) encompass military engagements that exclude direct combat, focusing primarily on humanitarian assistance, disaster relief (HADR), and peacekeeping initiatives. The integration of IoT devices holds significant promise in enhancing the effectiveness of such operations. For example, deploying autonomous drones linked to central command centers can pinpoint areas requiring assistance and facilitate targeted rescue and relief efforts. This approach minimizes the risk of futile missions and reduces exposure to hazards for rescue teams. Similarly, IoT devices operating in hazardous zones during HADR operations can mitigate risks effectively. Deploying IoT devices in volatile areas during peacekeeping missions increases safety and improves operational efficiency [57]. The convergence of IoT with advanced technologies like Artificial Intelligence (AI) is poised to transform military systems, potentially reducing reliance on large military forces. Automation facilitated by IoT-connected systems could replace human personnel in battlespaces, leading to

cost efficiencies through streamlined operations and reduced maintenance expenditures on autonomous platforms compared to personnel costs. Military establishments and governments increasingly favor this strategic shift globally. For example, defense organizations are shifting away from human resources and adding more capabilities through the application of sophisticated military technologies that demonstrate the general tendency of organizations to increase modernity and reliance on artificial intelligence.

Emerging research highlights the shifting nature of military operations other than war stressing the critical need for coordinated action between armed forces and civilian agencies to effectively manage and mitigate disaster scenarios. Research highlights the critical need for joint training and cooperation to bolster disaster management capabilities. There is growing recognition of the multifaceted nature of MOOTW, necessitating analyses that incorporate economic, political, social, and cultural dimensions. This paradigm shift calls for specialized training for analysts to effectively navigate complex MOOTW scenarios. The military's involvement in humanitarian endeavors, such as famine relief in Somalia and efforts to restore stability in Haiti and the Balkans, illustrates MOOTW's expanding role in addressing global crises. These advancements underscore the evolving complexity of MOOTW operations and underscore the importance of ongoing adaptation and collaboration between military and civilian entities [58][59].

Lethal Autonomous Weapon Systems (LAWS):

The integration of Lethal Autonomous Weapon Systems (LAWS), empowered by Artificial Intelligence (AI), is going to disrupt the military IoT game plan shortly. Despite all the ethical arguments and technical discussions among scientists and representatives of defense ministries, there is an evident consensus towards the inclusion of offensive LAWS in future military operations. Various defense sectors are investing in autonomous weapon systems, integrating AI to enhance decision-making speed and precision in response to battlefield dynamics. These systems, including drone swarms and robotic units, reduce human exposure to high-risk scenarios, allowing for rapid response times and efficient operational control. Ethical and legal considerations continue to shape the development and deployment of such technologies within defense frameworks globally. Effective deployment of LAWS in military IoT systems is important to achieve coordination on the battlefield.

The advancement in LAWS remains a research and discussion topic among military and international law circles. As advancements in LAWS continue, they have become a focal point of ongoing research and debate within military and international law circles. For example, "Killer Robots" use Artificial Intelligence and autonomous technology, to choose targets and launch an attack without human intervention [56]. It is believed that its appearance will lead to revolutionary improvements in warfare, which will give rise to new evolutionary steps as well as outstanding ethical problems.

Concerns about the political and moral acceptability of weapons independently have led to arguments for proper control and regulation, as well as the creation of new international laws to govern the development and deployment of lethal weapons. Concerns regarding the ethical implications of granting autonomy to weapons have spurred calls for stringent regulations and international legal frameworks to govern their development and deployment. Ethical dilemmas arise with the more use of robotics, it will also raise concerns about the LAWs deciding casualties of human beings. Thus, undermining conventional aspects of accountability and responsibility in warfare. For example, whereas the EU has a unified and clear position demanding the full elimination of LAWS, the leading powers of the world like the USA, China, and Russia, of course, take the position that seeks to reconcile military security concerns with those of regulation [60]. Current debates such as in the UN Convention on Conventional Weapons, identify the amount of human control required for the legal deployment of LAWS [60].

Humanitarian organizations and activist coalitions advocate for robust ethical frameworks governing military engagements to safeguard civilian populations and uphold international humanitarian principles in conflict areas. Despite the potential advantages of laws, substantial challenges remain in ensuring the deployment of these laws, highlighting the difficulties of ethical and legal implications in contemporary war zones. Ultimately, addressing these ethical concerns is challenging to a framework that manages a balance between the innovation of new technologies in the military with more accountability and international stability.

The Connected Combatant:

Soldiers their weapons and armored vehicles are connected through wired and wireless mediums to exchange information. Shortly, advanced technologies will enable the integration of sensors into combative weapons that will also capture the medical health of soldiers with real-time data apart from communication, positioning, and logistics as well as weapon status. From this capability, decisions about soldiers' rest and replacement, battalion health, and timing for the next operations will made. IoT will improve soldiers' situation awareness and identification, while augmented reality technologies will allow soldiers to order artillery and air support through handheld devices, key information from which will automatically transmitted to IoT platforms.[26].

Future aerial missions envision manned and unmanned aircraft flying in coordinated formations facilitated by IoT, potentially replacing costly military systems with more cost-effective autonomous technologies leveraging drone-swarming capabilities. IoT integration of Intelligence, Surveillance, and Reconnaissance (ISR) devices tailored to specific missions could enhance counterinsurgency efforts.

AI and IoT-based technologies in the battlespace will provide real-time situational awareness and scenario simulation, even in complex, rapidly changing environments with vast data volumes. This capability allows commanders to visualize integrated battlefields, focus on critical areas, and simulate scenarios realistically using 3D virtual reality technologies. These systems will also incorporate ambient factors such as weather and chemical data [14]. Recent advancements in the Connected Combatant for 2024 include the development of networked battle command systems aimed at enhancing joint fires for combatant commanders [56]. Studies on combat athletics highlight the crucial role of dynamic opponent interactions prompting fighters to adaptively form effective tactical coordination and exploit situational instabilities to maximize competitive advantages and overall performance outcomes. Defense research emphasizes fusion technologies to enhance underwater warfare effectiveness through networked information sharing, exemplified by the Networked Enabled Combat System (NECS). Developments in cross-species sequence alignment programs like COMBAT enable efficient comparison of vertebrate genomes, thereby enhancing genomic analysis capabilities [59]. Lastly, critical technologies for fighter aircraft in networked combat include time registration processing, data latency management, and the establishment of a standardized guidance coordinate system to facilitate effective target information transmission [61].

Conclusion:

The Internet of Things (IoT) is the latest innovation in this era. In some areas of military technology, most types of sensors, vehicles, and nuclear and chemical weapons seem unlikely to change dramatically. But perhaps a true military revolution will occur even without such developments with the help of IoT. Any Country can implement this technology in the defense sector to improve defense strategies against any harmful activity and make a strong, secure defense system. Proper research work for improvement in the conventional structure of defense systems into the latest structure of defense systems is needed. Suppose the stockholders of government and experts will start the research on transforming all dimensions of armed forces defense system into IoT technology and other latest technologies. In that case, this is very

important for the country's future defense. We can also find the solutions for the security and privacy of all data of the system, implementation of IPV6 over IPV4, development the intelligent AI-based network for IoT devices and sensors, and decide the way of IoT, vehicle-to-vehicle communication and connectivity of military assets in a warzone for future military and country's security activities in a synergistically way.

Acknowledgment: The authors here would like to acknowledge the resources and support of the respective academic institutions. No help from other sources has been taken in the preparation of this manuscript.

Author's Contribution: Corresponding author Naila Latif contributed to the conceptualization, writing, and revision of the manuscript. Muhammad kashif as the first author contributed to data collection, review of the related literature, writing, and critical analysis of the studies included in this review article.

Conflict of Interest: Authors declared that there is no conflict of interest in publishing this manuscript in IJIST.

Project Details: This research was not conducted as part of a specific project with external funding.

References:

[1] Y., Tertyshnik., O., Potapov., A., Mishok., A., Andrushko. (2024). 4. Analysis of the possibilities of using iot for military purposes. Zbìrnik naukovih prac′ Deržavnogo naukovo-doslìdnogo ìnstitutu viprobuvan′ ì sertifikacìï ozbroênnâ ta vìjs′kovoï tehnìki, doi: 10.37701/dndivsovt.19.2024.17

[2] D. E. Zheng and W. A. Carter. Leveraging the Internet of things for a more efficient and effective military. Rowman & Littlefield, 2015.

[3] Defense Technical Information Center. A Vision toward an Internet of Battlefield Things (IoBT): Autonomous Classifying Sensor Network. 2018. Retrieved from https://apps.dtic.mil/sti/tr/pdf/AD1064107.pdf

[4] Jamal, Alotaibi., Lubna, Alazzawi. (2020). 1. Insight into IoT Applications and Common Practice Challenges. International Journal of Trend in Scientific Research and Development,

[5] Y. Zhang, N. Meratnia, and P. Havinga. Outlier detection techniques for wireless sensor networks: A survey. IEEE Communications Surveys & Tutorials, 12:159–170, 2010.

[6] Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A literature review. Journal of Computer and Communications, 3(5), 164-173.

[7] Georgios, L., Kerstin, S., & Theofylaktos, A. (2019). Internet of things in the context of industry 4.0: An overview.

[8] M. A. N. U. Ghani, K. She, M. A. Rauf, S. Khan, J. A. Khan, E. A. Aldakheel, and D. S. Khafaga. Enhancing Security and Privacy in Distributed Face Recognition Systems through Blockchain and GAN Technologies. Computers, Materials & Continua, 2024.

[9] Munir, Arslan, Alexander Aved, and Erik Blasch. "Situational awareness: techniques, challenges, and prospects." AI 3.1 (2022): 55-77.

[10] N, Ghani., Aznida, Abu, Bakar, Sajak., Rehan, Qureshi., Megat, F., Zuhairi., Zaid, Mujaiyid, Putra, Ahmad, Baidowi. (2024). 1. A Review of Fog Computing Concept, Architecture, Application, Parameters and Challenges. JOIV : International Journal on Informatics Visualization, doi: 10.62527/joiv.8.2.2187.

[11] Nichols, R. K., Mumm, H., Lonstein, W. D., Ryan, J. J., Carter, C. M., Hood, J. P., ... & Jackson, M. J. (2020). Unmanned vehicle systems & operations on air, sea, land. New Prairie Press.

[12] Gunn, L. J., Asokan, N., Ekberg, J. E., Liljestrand, H., Nayani, V., & Nyman, T. (2022). Hardware platform security for mobile devices. Foundations and Trends® in Privacy and Security, 3(3-4), 214-394.

[13] M. A. N. U. Ghani, K. She, M. A. Rauf, M. Alajmi, Y. Y. Ghadi, and A. Algarni. Securing synthetic faces: A GAN-blockchain approach to privacy-enhanced facial recognition. Journal of King Saud University-Computer and Information Sciences 36(4): 102036, Elsevier, 2024.

[14] Ghani, M. A. N. U., She, K., Rauf, M. A., Khan, S., Khan, J. A., Aldakheel, E. A., & Khafaga, D. S. (2024). Enhancing Security and Privacy in Distributed Face Recognition Systems through Blockchain and GAN Technologies. Computers, Materials & Continua.

[15] N. C. Winget, A. R. Sadeghi, and Y. Jin. Invited: Can IoT be secured: Emerging challenges in connecting the unconnected. In Proceedings of the 53rd Annual Design Automation Conference, pages 1–6, New York, USA, 2016.

[16] H. Roberts, J. Cowls, J. Morley, M. Taddeo, V. Wang, and L. Floridi. The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. Springer, 2021.

[17] J. J. Kang. A military mobile network design: mhealth, iot and low power wide area networks. 2020.

[18] C. Chang, S. N. Srirama, and R. Buyya. Internet of things (iot) and new computing paradigms. In Fog and Edge Computing: Principles and Paradigms, volume 6, pages 1–23. 2019.

[19] D. Chethan, S. Bhuvana, and S. Kumar. Defense communication system aws. Applied and Computational Engineering, 2023.

[20] T. Sweijs, S. van Genugten, and F. Osinga, editors. Defence Planning for Small and Middle Powers: Rethinking Force Development in an Age of Disruption. Taylor Francis, 2024.

[21] M. Noura, M. Atiquzzaman, and M. Gaedke. Interoperability in internet of things: Taxonomies and open challenges. Mobile Networks and Applications, 24:796–809, 2019.

[22] J. Koo, S. R. Oh, S. H. Lee, and Y. G. Kim. Security architecture for cloud-based command and control system in IoT environment. Applied Sciences 10(3): 1035, MDPI, 2020.

[23] S. Kumari. Wearable brain computer interfaces (bci) in fog computing using wireless technology. 2023.

[24] Ricky, Rajora., Aarju, Rajora., Bhanu, Sharma., Priyanshi, Aggarwal., Siddhant, Thapliyal. (2024). 2. The Impact of the IoT on Military Operations: A Study of Challenges, Applications, and Future Prospects. doi: 10.1109/iciptm59628.2024.10563671

[25] Y., Tertyshnik., O., Potapov., A., Mishok., A., Andrushko. (2024). 1. Analysis of the possibilities of using IoT for military purposes. Zbìrnik naukovih prac′ Deržavnogo naukovo-doslìdnogo ìnstitutu viprobuvan′ ì sertifikacìï ozbroênnâ ta vìjs′kovoï tehnìki, doi: 10.37701/dndivsovt.19.2024.17

[26] S. V. Margariti, V. V. Dimakopoulos, and G. Tsoumanis. Modeling and simulation tools for fog computing—a comprehensive survey from a cost perspective. Future Internet 12(5): 89, MDPI, 2020.

[27] Hammoudi, S., Aliouat, Z., & Harous, S. (2018). Challenges and research directions for Internet of Things. Telecommunication Systems, 67, 367-385.

[28] (2022). 1. Case Study of Cloud Computing Security Issues and confidentiality Challenges. International journal of emerging trends in engineering research, doi: 10.30534/ijeter/2022/051042022.

[29] F. Wen, Y. Zheng, C. Yang, and W. Liu. Recent advancements in sensor technologies for healthcare and biomedical applications. Sensors, 2023.

[30] M. M. Sadeeq, N. M. Abdulkareem, S. R. Zeebaree, D. M. Ahmed, A. S. Sami, and R. R. Zebari. IoT and cloud computing issues, challenges and opportunities: A review. Qubahan Academic Journal, 1(2):1–7, 2021.

[31] US Department of Defense. Department of defense announces successful micro-drone demonstration, January 9 2017. Accessed on 20 April 2018.

[32] W. Yan, A. Fu, Y. Mu, X. Zhe, S. Yu, and B. Kuang. Eapa: Efficient attestation resilient to physical attacks for iot devices. In Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things, pages 2–7, 2019.
[33] Tan, W. C., & Sidhu, M. S. (2022). Review of RFID and IoT integration in supply chain management. Operations Research Perspectives, 9, 100229.
[34] A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou. A roadmap for security challenges in the internet of things. Digital Communications and Networks, 4(2):118–137, 2018.
[35] B. E. Katalin. Possibilities and security challenges of using IoT for military purposes. Hadmérnök 13(3): 378--390, 2018.
[36] Ghani, M. A. N. U., She, K., Rauf, M. A., Khan, S., Alajmi, M., Ghadi, Y. Y., & Alkahtani, H. K. (2024). Toward robust and privacy-enhanced facial recognition: A decentralized blockchain-based approach with GANs and deep learning. Mathematical Biosciences and Engineering, 21(3), 4165-4186.
[37] D. Araya and M. King. The impact of artificial intelligence on military defence and security. CIGI Papers, 2022.
[38] Y. Tadjdeh. Industry Ruggedizing, Securing Battlefield Radios. National Defense 102(771): 37--37, JSTOR, 2018.
[39] J. Danaher. Robot Betrayal: a guide to the ethics of robotic deception. Ethics and Information Technology 22(2): 117--128, Springer, 2020.
[40] I. Yaqoob, E. Ahmed, I. A. T. Hashem, A. I. A. Ahmed, A. Gani, M. Imran, and M. Guizani. Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges. IEEE Wireless Communications, 24(3):10–16, 2017.
[41] V. Tyurin, O. Martyniuk, V. Mirnenko, P. Open'ko, and I. Korenivska. General approach to counter unmanned aerial vehicles. In 2019 IEEE 5th International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD), pages 75–78. IEEE, October 2019.
[42] M. Bressan and G. Cuzzelli. From Clausewitz to Putin: War in the 21st Century: Reflections on Conflicts in the Contemporary World. 2024.
[43] S. S. Buchanan. Cyber-attacks to industrial control systems since Stuxnet: A systematic review. Capitol Technology University, 2022.
[44] R. Raman and L. Vyakaranam. Iot-enabled smart military training for virtual simulation and realtime performance analysis. In 2024 International Conference on Advances in Data Engineering and Intelligent Computing Systems (ADICS), pages 1–6. IEEE, April 2024.
[45] Sakthi P. and N. SatheeshKumar. Iot-based realtime system for tracking and monitoring the health of soldier. 2023
[46] David E. Sanger. Stuxnet worm was perfect for sabotaging centrifuges. The Hindu, 2010. Accessed on 6 May 2018.
[47] M. Tortonesi, J. Michaelis, N. Suri, and M. Baker. Software-defined and value-based information processing and dissemination in iot applications. In Network Operations and Management Symposium (NOMS), 2016 IEEE/IFIP, pages 789–793. IEEE, 2016.
[48] M. A. N. U. Ghani, K. She, M. A. Rauf, S. Khan, M. Alajmi, Y. Y. Ghadi, and H. K. Alkahtani. Toward robust and privacy-enhanced facial recognition: A decentralized blockchain-based approach with GANs and deep learning. Mathematical Biosciences and Engineering 21(3): 4165--4186, 2024.
[49] A. Sharma and S. Aggarwal. Real-time health monitoring system of soldiers using iot. In Advanced Computational Paradigms and Hybrid Intelligent Computing: Proceedings of ICACCP 2021, pages 285–296. Springer Singapore, 2022.
[50] Naresh Persaud. 2018 prediction: Securing iotconnected devices will be a major cybersecurity challenge. CSO, December 22 2017. Accessed on 20 May 2018.

[51] V. S. Sokolović and G. B. Marković. Internet of Things in military applications. Vojnotehnički glasnik 71(4): 1148--1171, Гачепа Небойпа Николаевич, 2023.
[52] A. Filipovi´c. Lethal autonomous weapon systems (laws): Towards global regulation or indiscriminate employment? Politiˇcka revija, 2023.
[53] Y. Gunawan, M. H. Aulawi, R. Anggriawan, and T. A. Putro. Command responsibility of autonomous weapons under international humanitarian law. Cogent Social Sciences 8(1): 2139906, Taylor & Francis, 2022.
[54] E. E. Nwabueze and O. E. Osuagwu. A model for predicting migration from ipv4 to ipv6 by 2027 in nigeria. Open Journal of Modelling and Simulation, 6(3):45–57, 2018.
[55] S. Tedeschi, D. Rodrigues, C. Emmanouilidis, J. Erkoyuncu, R. Roy, and A. Starr. A cost estimation approach for iot modular architectures implementation in legacy systems. Procedia Manuf., 19:103–110, 2018.
[56] N. Agrawal and A. Saxena. Artificial intelligence equipped edge internet of things (iot) devices in security. In Advanced IoT Technologies and Applications in the Industry 4.0 Digital Economy, page 296. 2024.
[57] Naresh Persaud. 2018 prediction: Securing iotconnected devices will be a major cybersecurity challenge. CSO, December 22 2017. Accessed on 20 May 2018.
[58] R. Hassan, F. Qamar, M. K. Hasan, A. H. Mohd Aman, and A. S. Ahmed. Internet of Things and its applications: A comprehensive survey. Symmetry 12(10): 1674, MDPI, 2020.
[59] N. Suri, G. Benincasa, R. Lenzi, M. Tortonesi, C. Stefanelli, and L. Sadler. Exploring value of information-based approaches to support effective communications in tactical networks. IEEE Communications Magazine, 53(10):39–45, October 2015.
[60] K. Velasquez, D. P. Abreu, M. Curado, and E. Monteiro. Service placement for latency reduction in the internet of things. Annals of Telecommunications, in press.
[61] G. S. Hukkeri and R. H. Goudar. Iot: Issues, challenges, tools, security, solutions and best practices. International Journal of Pure and Applied Mathematics, 120(6):12099–12109, 2019.
[62] Ghani, M. A. N. U., She, K., Rauf, M. A., Alajmi, M., Ghadi, Y. Y., & Algarni, A. (2024). Securing synthetic faces: A GAN-blockchain approach to privacy-enhanced facial recognition. Journal of King Saud University-Computer and Information Sciences, 36(4), 102036.
[63] B. Nikhil, H. Gaikwad, K. Smith, H. Khare, R. Ugale, D. Mendhe, V. Tiwari, A. Bajaj, and G. Keskar. Hardware design and implementation of multiagent mlp regression for the estimation of gunshot direction on iobt edge gateway. IEEE Sensors Journal, 2023.
[64] Payal, M., Dixit, P., Sairam, T. V. M., & Goyal, N. (2021). Robotics, AI, and the IoT in defense systems. AI and IoT-Based Intelligent Automation in Robotics, 109-128.
[65] Nilchiani, R. R., Verma, D., & Antón, P. S. (2023). Joint All-Domain Command and Control (JADC2) Opportunities on the Horizon. Acquisition Research Program.
[66] Wójtowicz, T., & Król, D. (2018). Multi-domain battle: new doctrine of the United States Armed Forces. Zeszyty Naukowe Akademii Sztuki Wojennej, (3 (112), 64-78.
[67] Greenley, H. L. (2019). Department of defense energy management: Background and issues for congress. Congressional Research Service, Washington, DC.