IJECBE

IJECBE (2025), **3**, **1**, 157–187
Received (16 April 2025) / Revised (25 April 2025)
Accepted (29 April 2025) / Published (30 May 2025)
https://doi.org/10.62146/ijecbe.v3i1.112
https://ijecbe.ui.ac.id
ISSN 3026-5258

International Journal of Electrical, Computer and Biomedical Engineering

RESEARCH ARTICLE

Transforming Humanitarian Response with IoT in Conflict Zones: Field Insights, Ethical Frameworks, and Deployment Challenges

Budi Dhaju Parmadi* and Kalamullah Ramli

Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia, Depok, Indonesia
*Corresponding author. Email: bparmadi@gmail.com

Abstract

The integration of Internet of Things (IoT) solutions into the delivery of humanitarian aid can be potentially transformative in improving the effectiveness of operations, time management, and the logistical performance in conflict-affected environments. However, there are some critical challenges, which include poor infrastructure, limited and irregular network coverage, increased cyber security risk, and cultural issues. Even though most of the existing literature focuses on these issues separately, this thematic review uses thematic analysis of peer-reviewed literature and humanitarian field reports and documented case studies, is the first to offer an integrated review of the infrastructural, security, and ethical aspects of IoT implementation simultaneously. This review reveals new approaches; decentralized IoT architectures, blockchain-secured networks, AI-assisted data analysis, and alternative network architectures. It focuses on ethical governance, addressing technocolonial issues, fair data management, and design for communities. The research presents a field-informed challenge–solution matrix and assesses ethical safeguards through IEEE Ethically Aligned Design (EAD) guidelines and the Ethics Canvas. The research provides practical recommendations which enable researchers and policymakers and practitioners to deploy IoT systems that are resilient and scalable and ethically responsible while establishing future directions for sustainable governance and inclusive humanitarian innovation.

Keywords: Internet of Things (IoT), Humanitarian Aid, Conflict Zones, Ethical Frameworks, Field Deployment

1. Introduction

The integration of Internet of Things (IoT) technology is revolutionizing aid delivery and logistics management and setting new standards for efficient resource allocation in humanitarian operations. IoT enables real time tracking, predictive analytics and automated decision making that improves situational awareness and response efficiency in crisis settings. However, deployment in conflict zones is accompanied by several challenges, including damaged infrastructure, limited connectivity and increased security risks [1].

These obstacles must be addressed to fulfill the maximum IoT potential in aiding the delivery of goods. Although prior studies have highlighted technological innovation in humanitarian logistics, very few have provided an integrated examination of IoT adoption that specifically addresses infrastructural, security, and ethical dimensions simultaneously. This thematic review fills this critical gap by systematically reviewing recent literature to present a holistic picture of IoT implementation challenges and solutions for IoT implementation, with a unique focus on ethical governance and socio-cultural factors. Therefore, this article aims to:

- Analyse key weaknesses and deficiencies of existing IoT solutions for humanitarian aid
- Assess possible new ways of developing IoT in the future.
- Suggest best practices for building sustainable and expandable IoT systems in humanitarian missions.

This article provides a clear and structured approach of how the reader will be guided from the basic concepts and background information to the specific thematic issues and practical suggestions. First, the introduction explains the role and importance of IoT in humanitarian aid in conflict areas and its challenges. Then, the methodology section explains in detail how the study employed a systematic approach to article selection and thematic analysis. Other sections provide a detailed analysis of the themes, which include examining constraints on the infrastructure, cybersecurity risks, interoperability problems, and socio-cultural barriers, each of which is followed by suggested innovative solutions. The article ends with a conclusion of major implications and a set of specific recommendations for future work, thus offering a systematic approach for the effective and responsible use of IoT in humanitarian settings.

1.1 Challenges in IoT Deployment in Conflict Zones

To better understand the severity of issues facing the implementation of IoT in conflict zones, Figure 1 provides a comparison of the different barriers, and their impact ranked from severe to least severe.

The radar chart presents a quantitative analysis of the key barriers to the adoption of IoT in humanitarian settings. Six primary challenges: Infrastructure Limitations, Connectivity Barriers, Cybersecurity Vulnerabilities, Standardization Issues, Ethical & Privacy Concerns, and Adoption & Cost Barriers are identified as the greatest constraints [2], [3], [4], [5]. Infrastructure Limitations (9/10) are the worst, based on damaged communication networks, unstable power grids, and limited hardware availability in conflict zones [6], [7]. Cybersecurity Vulnerabilities (9/10) are a critical

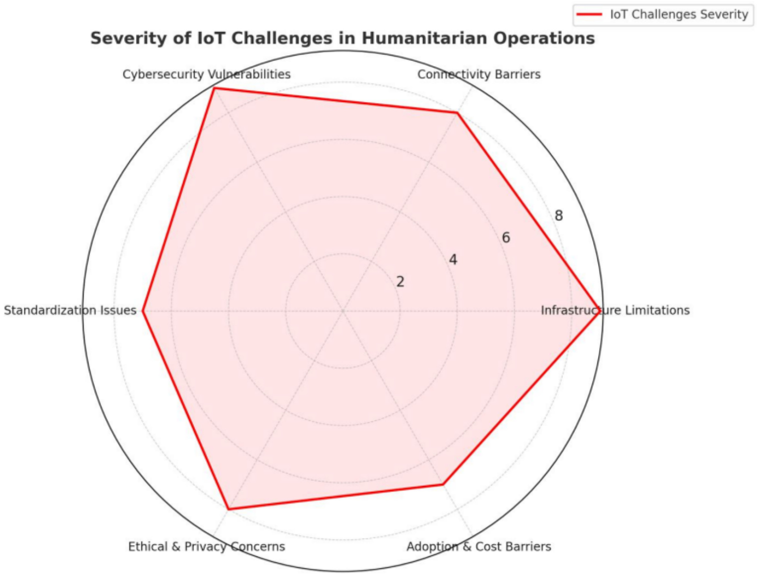

Figure 1. IoT Challenges in Humanitarian Operation

threat due to cyberattacks, unauthorized access, and data breaches that can compromise sensitive information and halt aid logistics [8], [9]. Connectivity Barriers (8/10) highlight the weakness of traditional network infrastructure, which is especially unstable in remote or high-risk regions, where real-time data exchange is unreliable [6], [10]. Ethical & Privacy Concerns (8/10) emphasize the risks of data misuse, unauthorized surveillance, and geopolitical sovereignty conflicts, particularly in refugee monitoring and medical aid applications [9], [11].

Impaired Infrastructure: Many conflict-affected regions see substantial degradation of power grids, communication networks, and transportation systems, obstructing the deployment of IoTenabled sensors, tracking devices and network nodes [2], [11]. The lack of reliable infrastructure is a considerable challenge to maintaining a continuous data flow and operational efficiency [1], [2], [12].

Limited Connectivity: IoT systems rely on uninterrupted data exchange to monitor aid distribution, security threats, and population movements [2], [9], [11]. However, unstable or absent internet access in conflict zones disrupts communication between IoT devices, field teams, and command centers, reducing real-time decision-making capabilities and delaying critical interventions [1], [13]

Security Vulnerabilities: IoT implementations in high-risk settings are susceptible to cyberattacks, unlawful access, and physical threats [9]. It is imperative to implement data encryption, secure communication, and robust system architecture to safeguard relief workers, beneficiaries, and sensitive information, including geolocation data of convoys and medical records, from potential exploitation [14], [15].

1.2 Innovation and Solution

Enhancing the existing IoT security frameworks with end-to-end encryption [9], blockchainbased [6] data verification and IDS that are AI driven [9] can secure the sensitive humanitarian data and increase the system robustness to cyber threats.

Humanitarian Flying Warehouse (HFW) [16]: Unmanned Aerial Vehicles (UAVs) that are integrated into IoT logistics systems can avoid the limitations of ground-based infrastructure and provide on-time delivery of medical supplies, food and emergency assistance to remote regions [17], [18]. These autonomous UAV networks provide continuous, adaptive supply chain management, even in highly volatile environments.

Digital Health Solutions: IoT-enabled healthcare innovations, including wearable diagnostic gadgets, telemedicine platforms and AI-driven disease monitoring, improve medical service accessibility in conflict zones [2]. The collection of real-time patient data enhances emergency response coordination and optimizes resource usage, even in regions with little healthcare infrastructure [2], [19].

Public Private Partnerships (PPPs): Relationships between humanitarian organizations, governments and technology vendors are crucial for increasing the deployment of IoT, funding and sustainability [20]. However, these partnerships must be designed to avoid power relations and for ethical, equitable technology deployment that ensures data governance, resource distribution, and capacity building are in line with humanitarian principles [20]

As IoT solutions are to be used in humanitarian settings, it is important to deal with issues such as lack of infrastructure, connectivity, and security threats. Secure IoT integration, UAV-based logistics, and digital health innovations, with the help of multistakeholder partnerships, can improve coordination of aid, resilience of operations, and efficiency of response. Future work and investment should be sustainable, flexible, and community-oriented IoT deployments to ensure that the technologies are used to their full potential with minimal risks in humanitarian crises.

2. Methodology

This thematic review follows a systematic approach of PRISMA (Figure 2) to synthesize critically current literature and the latest advances of IoT solutions for humanitarian aid delivery in conflict zones. The systematic methodological process involved the rigorous selection of peerreviewed journal articles, technical reports, and policy documents published between 2019 and 2024. Literature was retrieved from IEEE Xplore, Scopus, Web of Science, and Google Scholar using targeted search combinations of keywords such as 'IoT,' 'humanitarian aid,' 'conflict zones,' 'cybersecurity,' 'connectivity', and 'decentralized systems.'

The initial search yielded a rich collection of sources, and 75 references were chosen from rigorous inclusion criteria of works that discussed not only innovations and practical applications of IoT but also limitations and contextual challenges specific to conflict-affected regions. The thematic analysis mainly focused on literature published between 2021 and 2024, when the literature surged forward due to growing interest and improvements in IoT technologies.

From the total references, 20 publications constituted the core analytical foundation as they were the most in-depth, relevant, and frequently cited across the thematic

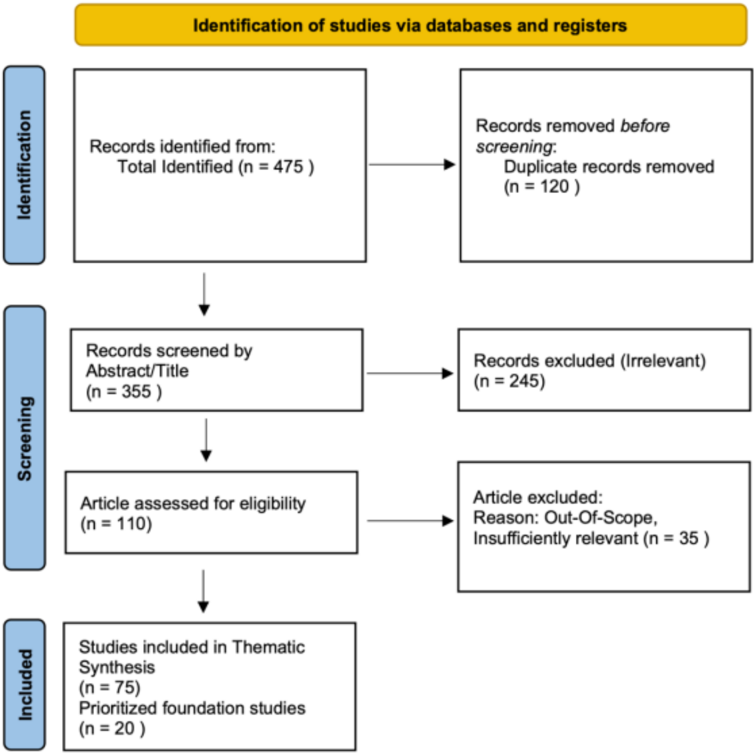
Identification of studies via databases and registers
Identification
Screening
Included
Records identified from:
Total Identified (n = 475)
Records removed *before screening*:
Duplicate records removed
(n = 120)
Records screened by Abstract/Title
(n = 355)
Records excluded (Irrelevant)
(n = 245)
Article assessed for eligibility
(n = 110)
Article excluded:
Reason: Out-Of-Scope,
Insufficiently relevant (n = 35)
Studies included in Thematic Synthesis
(n = 75)
Prioritized foundation studies
(n = 20)

Figure 2. PRISMA Flowchart on Literature Selection for Thematic Synthesis

synthesis. Some of the most heavily cited works are blockchain-enhanced IoT security studies [21], [22], [23], AI-driven analytics for network optimization and cybersecurity [24], [25], [26], decentralized communication solutions [10], [27], satellite communication and connectivity and their limitations [28], [29], [30], ethical and governance frameworks [20], [31], [32], Cultural implications and techno-colonial concerns [33], [34], [35], privacy-preserving humanitarian digital wallet [36], and transparency and logistic sustainability [7].

The literature is mainly for 2020-2024, and the most important contributions were made between 2022 and 2024. After screening and evaluation, the selected literature was systematically analyzed to derive in-depth insights into infrastructure constraints, security vulnerabilities, interoperability challenges, and socio-cultural barriers. They then critically examined innovative IoT approaches like mesh networking, blockchain, AI-driven predictive analytics, and decentralized data processing.

This thematic review ensures a comprehensive and critical knowledge synthesis, using methodological rigor to produce actionable insights and strategic recommendations tailored to stakeholders deploying and governing IoT in humanitarian settings.

3. Thematic Analysis

This paper uses a systematic approach to synthesizing the primary challenges encountered in implementing IoT solutions for humanitarian aid in conflict zones and offers a more in-depth look at infrastructural challenges, security and privacy risks, standardization and interoperability challenges, and socio-cultural barriers. It also examines the innovative IoT technologies and practical approaches to solve these challenges and links the limitations identified to potential solutions to help guide the implementation of future systems.

3.1 Infrastructure Challenges

The deployment of IoT solutions in conflict zones is restricted by infrastructure limitations, primarily unstable internet connections, security threats, and weaknesses of centralized systems. These challenges hamper the efficiency of IoT-based humanitarian operations in terms of realtime data transmission, security, and resilience.

As pointed out in [6], [10], a major issue is the unreliable internet connectivity in conflict-affected areas. Some IoT applications rely on cloud computing for data analysis, control, and planning, but such networks are not reliable in areas with limited or no connectivity at all. This limitation hampers real-time monitoring of relief distribution, medical supplies, and situation awareness, which adversely impacts the effectiveness of humanitarian response [6], [10].

Security and privacy issues are the other factors that are major issues in the adoption of IoT technologies in these areas [9], [37], [38]. IoT devices gather and convey sensitive information such as location and the recipient of the assistance, which if intercepted, may be risky to vulnerable groups [9], [37]. Securing IoT networks is especially difficult in the compromised infrastructure of conflict zones. Encrypted communication, device authentication and a strong cybersecurity framework are critical to address the risks posed by adverse actors [34].

Another weakness is the conventional centralized systems usually applied in humanitarian logistics. The lack of integration among the actors and the possibility of system crashes only worsens the operational disturbances. In conflict zones where the infrastructure is usually unstable, decentralized or hybrid models based on edge computing and blockchain are more sustainable [21], [39], [40]. These approaches decrease the dependency on cloud computing by processing data at the edge and thus improving security and efficiency [21].

Beyond the issues of connectivity and security, power supply disruptions impair the functionality of IoT in a big way. Power is a critical factor in the real-time monitoring and control, data transport, and security aspects of the IoT, yet many affected regions experience power infrastructure destruction and energy source restriction [9], [10]. It has been identified that power outages are frequent, and they affect the performance of IoT operations, which include efficient distribution of aid, tracking of diseases, and response to emergencies [10].

The availability of power is a significant factor that limits the continuity of usage of IoT devices. In addition, access to backup power, such as solar panels or generators, is also limited due to access and security issues [10]. Without suitable alternative energy, humanitarian coordination with the aid of IoT becomes unreliable. Furthermore, power changes can affect the security of IoT platforms and make them vulnerable to cyber-attacks [8]. System integrity is also compromised by power failures since it leads to data leakage and non-delivery of important information and thus reduces the performance of the system [9]. System integrity is also compromised by frequent power outages, which results in data transmission failures, the loss of important information, and a decrease in performance [9].

Satellite networks are believed to solve IoT-driven humanitarian aid; however, all of them have certain drawbacks, including high costs, limited bandwidth, and low efficiency [29]. The costs of satellite communication, including spectrum and infrastructure, are also a deterrent. In addition, satellite architectures are not designed to support high-rate data flow, which affects real-time surveillance and relief operations. Power inefficiencies worsen these constraints since satellite terminals cannot sustain the transmission of large data over time [29], [30].

Latency problems are caused by bandwidth limitations, which are a problem for time-critical IoT applications like tracking of medical supplies and disaster management. Some IoT devices work with the help of the cloud, and constrained bandwidth results in increased latency and reduced performance [30]. However, scalability is still an issue since the number of IoT devices that can operate at the same time in conflict zones is limited by the available satellite bandwidth [28].

These infrastructure challenges can only be met by adopting a holistic strategy with robust network designs, strong security, and decentralized approaches. Optimizing bandwidth, integrating energy-efficient satellite technologies, and using hybrid connectivity approaches, such as a combination of satellite links, mesh topologies, and edge computing, will also be necessary to support the long-term deployment of IoT solutions for populations affected by conflict.

3.2 Security and Privacy Concerns

The use of IoT solutions in conflict zones is risk-prone in terms of security and privacy due to unstable infrastructure, the sensitivity of the data collected, and the lack of sufficient protective measures [33], [41]. These vulnerabilities can jeopardize cyber threats on humanitarian operations that include data breaches, device manipulation and unauthorized surveillance that may compromise the safety of the affected populations and hamper the delivery of aid [33], [41].

One issue raised is data sensitivity and security. Humanitarian IoT systems are critical in documenting the real-time locations of personnel, aid assets, and supply chains [9], [33]. Without strong encryption and access control, these devices are attractive cyber threat targets [2], [38]. A compromised IoT system can halt aid logistics and put the safety of humanitarian workers and vulnerable communities at risk [9], [33].

The challenge to network security in conflict zones is higher due to instability in connectivity and increased digital threats [9], [36], [38]. The lack of advanced security protocols makes IoT deployments vulnerable to cyber intrusions, interception, and manipulation [9], [38]. Attackers can gain access to weak authentication, compromise data integrity and even shut down IoT networks, disrupting critical operations [33], [42]. Because of these risks, it is crucial to have resilient network protocols and end-to-end encryption to ensure the integrity of the system and the security of the information.

Another significant problem is the issue with location privacy, as many IoT devices monitor the movement of humanitarian workers and aid convoys [33], [37], [41]. Although such data is essential for the security of operations and improving logistical performance, it can also be misused [41]. Adversaries could use location metadata to track humanitarian movements and thus expose personnel and beneficiaries. These methods are crucial to hide tracking patterns, while mix-zones and differential privacy techniques are used to make aid operations transparent and effective [41].

Thus, the limitations of the infrastructure in the conflict zones only increase the security risks. This paper has highlighted how poor or damaged network infrastructure hinders the adoption of comprehensive cybersecurity practices by exposing IoT devices to unauthorized access [6], [20]. The absence of standard security practices in humanitarian organizations also leads to different levels of protection, which are vulnerable to exploitation [6], [7]. To enhance the security of IoT devices in such conditions, it is necessary to have solution propositions that can be easily scaled up across the network, including decentralized authentication systems, hardware security modules, and secure firmware updates [6], [7].

In addition to the technical issues, ethical and privacy issues are raised by the big data collected in the context of sensitive humanitarian situations [9], [20], [43]. IoT-enabled humanitarian assistance generates vast data on refugees, medical supply chains, and crisis management. In the absence of adequate legal regulation and appropriate management of the data, the information may be misused by the state and non-state actors [6], [20], [31], [44]. Another ethical issue is the lack of consent processes which raises questions on how the affected populations are going to be affected by the data collection, storage, and sharing [6], [7], [20].

A significant issue in the application of IoT in humanitarian operations is techno-colonialism and power relations which see digital technologies being used to advance the agenda of certain stakeholders while at the same time exposing vulnerable populations to more risks [20], [45]. A significant concern is the centralized data power of international organizations, which is often exercised without adequate local participation [20], [31]. As noted earlier, proper management of data is crucial for the prevention of negative impacts and the appropriate implementation of IoT technologies in humanitarian operations [6], [7], [20], [46].

The examined models of IoT-based humanitarian assistance are characterized by weak encryption and authentication due to the costs, simplicity of operation, and lack of cybersecurity expertise at the humanitarian organization [9], [38]. This paper finds that many IoT devices deployed in resource-constrained environments do not have the necessary technical support to enforce strong security controls [9], [33], [47]. The dynamics of conflict zones make it hard to set standard security policies for various networks and devices [9], [47], [48].

Currently, existing IoT security frameworks in humanitarian contexts are inadequate [4], [49], which do not pay enough attention to the issue of data protection. Many devices have poor or old authentication mechanisms that can be easily compromised and manipulated [33], [42]. The absence of universal security standards results in fragmented protections [50], [51], resulting in inconsistencies that pose a greater risk of system breaches [49]. Hence, absence of a unified security approach, IoT enabled humanitarian efforts are prone to cyber exploitation and thus weak.

These security and privacy challenges can only be solved by a comprehensive cybersecurity strategy with standardized security frameworks, capacity building for humanitarian organizations and encryption technology investment. Secure-by-design IoT architecture development [20], privacy-enhancing technologies enablement [20], [36], and compliance with regulations are important steps to secure humanitarian aid operations from cyber threats. Thus, cybersecurity resilience is critical to the safe and effective deployment of IoT solutions in conflict-affected regions [9].

3.3 Standardization and Interoperability

It is crucial to ensure standardization and interoperability of IoT technologies on a global level for effective and efficient humanitarian aid delivery, especially in conflict zones where different technologies and stakeholders must work in harmony [6], [10], [27]. These frameworks enhance responsiveness, flexibility, and risk management by integrating IoT, blockchain, and open-source standards, thereby improving the efficiency of humanitarian logistics and governance [6], [7], [44], [52].

Global IoT frameworks enable the seamless integration of different systems and, in turn, the realtime interaction between NGOs, government agencies, and local communities [10], [20]. Standardized communication protocols and data formats enhance the efficiency of operations by increasing transparency and trust through secure and tamper-proof aid distribution [10], [27]. Furthermore, other technological advancements such as biometric identification [20], [32], the use of UAVs for the delivery of assistance [53], [54], [55], and big data analysis [55] have become more reliable and applicable when incorporated into a coherent regulatory system. Therefore, these improvements enable the victims of the crisis to exercise more control over the relief efforts and lessen the likelihood of being dependent on other actors

The implementation of open-source IoT standards enhances interoperability [27], security [6], and adaptability in rapidly evolving humanitarian crises [20]). These frameworks guarantee the standardization of data transmission protocols to enable the coordination of stakeholders while ensuring privacy and data integrity [6]. The integration of blockchain-based security measures guarantees secure and reliable transactions and helps to avoid fraud and corruption in humanitarian supply chains [6]. Moreover, open-source solutions empower communities as local actors can engage in the management of aid and thus ensure that solutions are people-centered [20].

Apart from the integration of technology, guidelines are important in the implementation of security in IoT applications in high risk areas [9], [27]. Standardized policies governed federated IoT ecosystems improve device onboarding security, data protection, and access control to enhance network and system [6], [10], [27]. Public private partnerships (PPPs) are crucial in enhancing the scaling of technological solutions, and regulations are important in ensuring that such collaborations are ethical and fair [20]. For instance, new digital health and humanitarian logistics applications like the humanitarian flying warehouse (HFW) cannot be implemented without proper regulations [20], [16].

It is therefore important to develop global IoT frameworks, open source standards and guidelines to support interoperability, security and governance of humanitarian operations across the world [9], [20]. These initiatives increase the credibility, productivity and robustness of the aid distribution process while providing communities with easily deployable and reusable IoT technologies [4], [20]. Future work should also involve improving the regulatory policies across sectors, integrating decentralized security mechanisms and enhancing the interoperability of shared data to sustain the effectiveness, ethics and technological soundness of IoT enabled humanitarian assistance in conflict zones [6], [20].

3.4 Comparative Analysis Humanitarian Cultural Barriers

Although IoT solutions present a great opportunity to enhance humanitarian aid processes, cultural and social factors create many problems [2], [35], especially in conflict areas where mistrust and technological naivete are barriers [2], [35]. People in local communities tend to view technological interventions as impositions rather than as enablers, which results in their opposition and skepticism [2], [35].

The biggest challenge is probably digital literacy and trust. Many communities in conflict-affected areas are not familiar with digital technologies and are therefore leery of IoT technology [2], [20]. Often, this skepticism is connected with a historical power imbalance, when external technological interventions brought more benefits to international stakeholders than to local populations and reinforced techno colonialism [20]. Besides, sovereignty issues come into play when the data and resources are controlled by external entities, something that is resisted by local authorities who do not want to be rendered powerless to prevent humanitarian operations [20].

Regulatory and knowledge barriers also hamper the adoption of IoT in humanitarian aid. The current absence of policies that govern the use of digital technologies in conflict zones creates uncertainty for both humanitarian organizations and local governments [35], [56]. For instance, in supply chain management, blockchain-based solutions could improve traceability and trust, but regulatory risk, knowledge issues and high costs have restricted their uptake [35]. Unless there is regulatory direction and support, including capacity building, the potential of IoT in aid logistics is underutilized [35], [56].

These barriers can be addressed through a community-focused approach that includes local people in the development and implementation of IoT solutions [20]. Thus, increasing educational and training levels can increase understanding and acceptance of the technology, which will help to increase trust. Furthermore, aspects such as data collection and usage transparency, which include the use of blockchain for verifiable records, can be used to gain the public's trust and improve coordination of aid distribution [6], [7], [35]. Important for sustainable adoption are culturally appropriate strategies that are compatible with local norms and priorities [20].

Besides the technical and regulatory issues, ethical issues are also crucial for the responsible use of IoT in the humanitarian setting. The privacy issues raised by the use of data collection, primarily in aid logistics and refugee movements [37], require strict governance frameworks [37]. If there are no clear policies on data ownership and consent, then IoT-enabled humanitarian operations may further expose the vulnerable rather than protect them [6], [20]. Furthermore, there are power relations in digital governance that have to be managed carefully so as not to take advantage [20]. If the data control is to be kept with the international actors and there is no equal local participation then the IoT solutions may only serve to perpetuate the systemic inequalities rather than the affected communities' empowerment [20]

The IoT innovations in humanitarian aid must also match the socio-cultural regions in order to be proper [20], [32], [57]. There are however, criticisms that have been made on some technological interventions such as biometric identification and drone based aid delivery as being neo-colonial in practice while at the same time claiming to empower locals [32]. In order to be sustainable, the humanitarian IoT applications should start from the local level and involve local people in the decision-making process rather than looking for universal solutions [20], [32]. This paper also notes that participatory design increases the likelihood of success of IoT solutions as it ensures that the solutions being harmoniously implemented are compatible with the needs and culture of the target population thereby increasing their acceptance and durability.

In order for IoT solutions to work in conflict zones they have to consider security, privacy [6], and cultural sensitivity [20] while overcoming limited infrastructure [6]. A proximity approach that includes the participation of community stakeholders [20], transparency [7], and adaptation to specific regional challenges [7], [58] is crucial for removing the barriers and ensuring the proper and ethical use of the IoT technologies [35], [58] in humanitarian aid. Thus, the principles mentioned above can be integrated to improve the performance of IoT solutions in supporting more effective, inclusive, and sustainable humanitarian operations in conflict-affected areas.

3.5 Innovative Connectivity Solutions

Building resilient and decentralized communication is important for IoT-enabled humanitarian operations, especially in conflict zones where conventional infrastructure has been destroyed [6], [7]. Mesh networks, Low-Power Wide-Area Networks (LPWAN), and AI-based optimization [10] enable real-time data communication, adaptive network topology, and better performance in highly dynamic conflict environments.

Wireless Mesh Networks (WMNs) are also used in ad hoc configuration to establish infrastructure with less connectivity, with the properties of auto-healing and self-configuration [59], [60]. Multi-hop topologies are used by WMNs to expand the coverage area; WMNs provide continuous connectivity even when fixed infrastructure is not available [59], [61]. Integration with LoRa enhances long-range network connectivity and enables IoT devices to transmit information over long distances with low power consumption [59], [62]. Moreover, the hybrid networks of LoRa, Bluetooth Mesh, and short-range ANT are also presented to supply power-efficient approaches for real-time position monitoring, data encryption, and efficient management of the humanitarian supply chain[59], [53].

Beyond static infrastructure, AI-based network optimization enhances IoT resilience by using machine learning algorithms for dynamic bandwidth allocation, predictive fault detection, and adaptive routing [6], [9]. This ensures network stability in the face of extreme dynamics. Furthermore, the integration of AI with blockchain technology improves trust, transparency, and security in the data-sharing processes, reducing the risks of manipulation and unauthorized access in crisis zones [6], [9]).

New innovative solutions in logistics and supply chain management, with the help of IoT sensors and aerial networks, contribute to the transformation of humanitarian connectivity. Real-time sensor integration for proactive health monitoring, environmental assessment, and supply chain tracking is a reality, which leads to more accurate aid delivery [6], [9]. The humanitarian flying warehouse, which uses autonomous UAVs, circumvents the need for ground-based infrastructure to fail and moves supplies into and out of hazardous zones safely and effectively [16].

The future of humanitarian IoT connectivity relies on improving adaptive network architectures, caching strategies, and strong security frameworks. The dynamic network management by the AI will predict the changes and make required changes to maintain the efficiency of data transmission even when the infrastructure is damaged. Decentralized caching mechanisms will enhance disaster preparedness by allowing the user to access important information even when there is no network access due to failure [6], [7], [10]. Also, new frequency-agile protocols like SPIDERMAN will enhance network reliability and reduce latency and interference in conflict environments [10], [20].

The integration of mesh networks, LPWAN, AI-driven optimizations, and blockchain security is transforming the way IoT is enabling humanitarian aid delivery [6], [7], [10]. These technologies provide reliable, scalable, and autonomous communication that enhances aid coordination, crisis response, and operational resilience. Future work should aim at extending the framework to include scalable security [6], intelligent resource allocation [7], and real-time adaptability [10] to make sure that the humanitarian response is data-informed, effective, and secure in the target areas.

3.6 Enhanced Security and Privacy Frameworks

Data security and privacy must be ensured in the context of humanitarian IoT deployments [24], [46], especially in conflict zones where cyber threats and unauthorized access pose severe risks. Blockchain technology [46], intrusion detection systems based on Artificial Intelligence (AI) [24], and Secure Multi-Party Computation (SMPC) [24] are robust for secure data sharing, network protection, and privacy-preserving computation in resource-constrained environments.

Blockchain technology improves trust, transparency, and security in humanitarian logistics by using decentralized storage, tamper-proof records, and smart contracts to reduce the risk of data breach and manipulation [6], [22], [58]. Attribute-based encryption (ABE) also improves key management and data access control to the finest level without the need to rely on centralized authorities, thus protecting health records, beneficiary identities, and aid distribution logs [23]. These mechanisms guarantee data integrity and verifiable transactions, in order to build trust and accountability in the coordination of the aid.

AI-based Intrusion Detection Systems (IDS) offers real-time threat detection and mitigation, thus overcoming the limitations of conventional security measures [26]. The machine learning algorithms facilitate the dynamic network defense analysis of the traffic patterns in order to detect and act on the cyber threats [25] that are likely to threaten humanitarian operations. In consequence, as IoT-based aid activities continue to grow, it is crucial to ensure the ethical use of data and compliance with privacy requirements in order to preserve the trust of the interested parties [9].

Secure Multi-Party Computation (SMPC) improves further privacy-preserving computation [63], to allow several parties to work with their data jointly without revealing their specific inputs. SMPC frameworks when embedded into IoT platforms secure digital identity verification, resource allocation, and financial aid distribution, all while preserving data privacy in hostile environments [64], [65]. Thus, SMPC is applicable to real-time, low-resource settings of humanitarian operations by means of optimized cryptographic methods such as Shamir's Secret Sharing [66] and homomorphic encryption ([67].

Vice versa, progress in the areas of blockchain security, AI-driven IDS, and SMPC is defining the improvement of humanitarian IoT ecosystems and enhancing the stability of operations in conflict zones. These innovations protect against cyber threats, ensure data accuracy, and uphold ethical standards for privacy to reinforce trust and effectiveness in the delivery of humanitarian aid. Future work should extend to the development of scalable cryptographic protocols, adaptive intrusion detection systems, and decentralized security architectures to enhance humanitarian IoT robustness in sensitive environments.

To address the operational challenges outlined across network, data, and ethical dimensions, the following Table 1, explaining field-validated mitigation framework synthesizes practical solutions documented in humanitarian deployments:

Table 1. Field-Validated Challenge Mitigation Framework for IoT Deployment in Conflict Zones

Challenge	Solution	Field Strategy
Low connectivity inwarzones	Hybrid LoRaWAN + Satellite Backhaul	Use local LoRaWAN for low-power transmission and satellite backhaul as fallback (e.g., Eutelsat trial in Mali).
Ethical uncertainty around data use	IEEE EAD + Ethics Canvas	Use ethical assessment tools during project design phase to anticipate misuse, improve transparency, and secure local consent.
Distrust of sensors among communities	Culturally adapted casing + consent icons	Replace "military-style" enclosures with neutral shapes and attach icons showing its function (e.g., water monitoring, not spying).
Sensor tampering or theft	Community-led device co- design and tamper alert systems	Involve local leaders in deployment decisions and deploy tamper alerts for critical infrastructure (e.g., chlorination monitors).
Short lifespan in harsh climates	Ruggedized devices + solar charging	Use enclosures with IP67 rating and include solar power kits adapted for dust, humidity, and extreme heat.

4. Discussions

This discussion synthesizes the practical implications of the thematic analysis and clearly states how identified challenges can be solved through actionable solutions. Each subsection explains how particular technological, regulatory, and socio-cultural innovations can address directly the specific challenges highlighted earlier, and thus to maintain the coherence and to show how IoT-enabled humanitarian aid delivery can become more resilient, efficient, and ethical in conflictaffected environments.

4.1 Integration and Interoperability

The disintegrated nature of IoT protocols restricts the interoperability among the humanitarian agencies, especially in the conflict zones, which makes coordination very essential for the purpose of delivering assistance [68]. The use of different communication protocols such as CoAP, REST, MQTT, and AMQP poses a challenge on the ease of use of integration with various IoT platforms, which hampers real-time communication and sharing of information among the humanitarian stakeholders [68]. The absence of the data normalization also increases the operational costs since different data formats lead to information silos and slow response in crisis situations [27], [68]. In practice, these fragmented standards demand more middleware and gateways, which only enlarge the technical complexity and the deployment costs. These challenges can be met by implementing multiprotocol platforms and standardized data representations in order to improve integration and achieve operational transparency and effective coordination of all humanitarian actions [27], [68].

These integration strategies are directly related to solving the previous challenge regarding the lack of interoperability and limited infrastructure in conflict zones. In this way, the communication protocols and data formats are unified to enable the exchange of information in real-time and increase the transparency of operations. The use of multi-protocol middleware and open-source gateways reduces the technical complexity of the system [27], [68] and thus solves the problems associated with infrastructure limitations identified in the thematic analysis.

4.2 Field Experiences from Humanitarian Deployments

The deployment of IoT systems in conflict areas depends on technical capabilities together with trust from local populations and sociopolitical support and ethical system design. The field evidence demonstrates that IoT solutions bring potential life-saving benefits, yet their implementation faces multiple security risks including connectivity weaknesses and system vulnerabilities and exclusion problems and moral challenges.

Water monitoring functions as a fundamental IoT system which operates in refugee settings. A UNHCR technologist stressed that maintaining clean water supply stands as a crucial measure to stop disease outbreaks. The UN operations installed Kerlink LoRaWAN gateways together with battery-powered sensors to track water levels in distant refugee camps without access to electricity [69].

Smart camps together with AI tools show how IoT systems can become effective when properly implemented. The UN Interim Security Force for Abyei (UNISFA) built a smart camp at Dokura/Rumajak through the implementation of UAV digital twins and wireless sensors which controlled water levels and automated environmental systems thus enabling staff to concentrate on essential needs [70]. The medical organization MSF has launched Antibiogo which uses AI to provide antibiotic recommendations through image-based susceptibility tests and operates in Mali, DRC, Jordan and Yemen [71].

The development of cyber protection measures occurs in parallel fashion. The ICRC together with 196 Geneva Convention signatories endorsed the digital emblem which serves as a cyber equivalent to the red cross to protect humanitarian systems from cyberattacks, Athough experts recognize that the symbolic protection does not stop deliberate ransomware attacks or state-sponsored cyber threats [72].

The current efforts to protect humanitarian systems have not eliminated the existing vulnerabilities which serious incidents continue to expose. Human Rights Watch documented in 2021 that UNHCR transferred Rohingya biometric information to Bangladeshi and Myanmar authorities even though Myanmar continued to persecute the Rohingya population [73]. The GPS spoofing incident in 2023 disrupted 20 civilian aircraft near Iranian airspace which caused concern about drone and convoy navigation systems in Syria and Iraq [74]. The AI tool “Where’s Daddy?” caused civilian deaths in Gaza through misidentification of targets based on mobile phone data because telecom infrastructure failures degraded its performance [75].

Surveillance tools experience violent misuse through physical infrastructure attacks. State forces bombed the MSF hospital in Old Fangak South Sudan after it received the designation of "hostile" area. The incident demonstrates how surveillance systems become weapons against humanitarian sites through geopolitical framing, yet it remains unclear if GPS or IoT systems were used for targeting [76]. The situation mirrors the same case as MSF did during the Syria crisis ten years ago when the organization ceased sharing its GPS location [77]

The combination of digital exclusion with structural risk makes these threats worse. The UNHCR reported that refugees who do not have devices or formal IDs experience systematic exclusion from digital services which leads to increased social marginalization and higher vulnerability to exploitation. The generation of incorrect data by misconfigured IoT systems leads to incorrect aid access and incorrect identification of individuals [78].

The period from 2023–2024 saw armed drones launch attacks against displacement camps and hospitals throughout Ethiopia Iraq and Myanmar. Surveillance and GPS-based navigation systems became targets for both state forces and non-state actors who used them to identify humanitarian convoys. The integration of drones into Internet-of-Drones (IoD) architectures creates rising security risks because GPS-dependent aid convoys in Ukrainian conflict zones were hit by missiles according to UNDSS reports [79].

The field evidence demonstrates that IoT represents more than a technical solution because it functions as a socio-technical system which exists within intricate ethical and cultural and political environments. The deployment of secure and inclusive systems needs ethical design frameworks like IEEE Ethically Aligned Design (EAD) and Ethics Canvas to build trust with communities and protect data and maintain operational legitimacy.

4.3 Security and Ethical Framework

The security issues in the IoT systems present severe risks to humanitarian operations because of the sensitivity of the data collected and processed; this includes information about the beneficiaries and the logistics of the operations [9], [20]. Practical implications are an increased risk of cyber attacks, data manipulation, and privacy violations that may disrupt aid operations and endanger the victims [20]. These risks are further worsened by the absence of universal security standards, which lead to the use of ad hoc and fragmented cybersecurity controls across humanitarian organizations. Security innovations such as the use of blockchain technology and AI-based intrusion detection systems are a direct consequence of the previously identified security vulnerabilities, which include poor data security and weak authentication [6]. Secure Multi-Party Computation (SMPC) and homomorphic encryption can be used by humanitarian organizations to handle beneficiary data in a safe manner, even in hostile environments, as identified previously [9].

In practice, strong security architectures, including blockchain, AI-based intrusion detection systems (IDS), and Secure Multi-Party Computation (SMPC), can be used to prevent threats and increase data and privacy security [6]. Moreover, adequately designed Public Private Partnerships (PPPs) could significantly help to solve the although they must be handled properly to avoid the potential of power imbalances and unethical data management technological and regulatory issues [20], [80], if transparently structured, could play a pivotal role in overcoming technological and regulatory barriers, yet these must be managed carefully to avoid power imbalances and ensure ethical, equitable data governance [20].

4.4 Humanitarian and Cultural Barriers

However, cultural and social factors continue to pose a significant threat to the adoption and effectiveness of IoT solutions. The digital divide and historical skepticism towards externally provided interventions create real challenges [20]. Techno colonialism concerns and local sovereignty concerns result in resistance to the successful implementation and adoption of new IoT technologies in conflict zones [20]. Practical measures that can be taken in order to overcome these barriers include digital literacy enhancement through capacity-building activities [56], a participatory design that is in harmony with the local community needs [20] and openness in communication [6], [7] In this way, culturally appropriate mechanisms [20] and equitable engagement of local populations in the decision-making process build confidence and lead to better accountability and ownership of IoT-related humanitarian action [7].

The effects of community-driven design and digital literacy practices are practical and can be used to tackle cultural barriers such as distrust and techno colonialism mentioned earlier [20]. The concept of participatory design, which involves the involvement of local people in the design process of IoT interventions, also helps in the ownership of the interventions and hence their acceptance [20], [51]. Other measures such as clear data governance frameworks that provide for data ownership and consent help to address ethical issues and thus decrease the likelihood of resistance from local stakeholders and increase their trust in humanitarian operations.

The study needs to create an ethical evaluation framework by integrating IEEE

Ethically Aligned Design (EAD) principles with the participatory Ethics Canvas methodology to systematically address ethical and cultural barriers. The framework consists of five fundamental dimensions which stem from these approaches: 1) Data Minimization, 2) Beneficiary Consent, 3) Do No Harm Risk Scoring (based on IASC's operationalization of Anderson's principle) [81], [82], 4) Stakeholder Accountability, and 5) Post-Deployment Review. The Safe Water Optimization Tool (SWOT) [83] from MSF showed the difference between Sphere Standards [82], [84] for water safety and the real situation in South Sudanese refugee camps during a hepatitis E outbreak. The tool's iterative design process, which combines data analysis and stakeholder participation, is in line with the ODI Data Ethics Canvas [84] by generating context-specific recommendations through localized risk assessments and feedback loops.

4.5 Emerging Innovations and Practical Implications

New technologies like blockchain [6], [7] and AI-driven analytics [7], [10] are potentially valuable to increase the accountability, transparency and performance of humanitarian logistics. Best, in practice, blockchain-based frameworks offer a clear record of aid distribution and thus reduce corruption risks and increase operational accountability [6], [7], [10]. AI-based predictive analytics help to improve the accuracy of the assessment of humanitarian needs and to act proactively during a crisis [7], [10]. Nevertheless, the actual usage of these technologies raises ethical issues such as bias in algorithms, privacy of data, and equity [6], [20]. Moreover, the use of biodegradable IoT sensors and decentralized logistics, including HFW that is based on UAVs also faces practical issues of scalability, regulatory compliance, and environmental friendliness [6]. To overcome these implementation barriers, there is a need for well-defined regulatory frameworks, open collaboration between the stakeholders and the constant ethical supervision to guarantee that the technological interventions are feasible and proportionate to the context.

4.6 Mapping Gaps to Solutions in IoT Deployment for Humanitarian Aid in Conflict Zones

Challenges of IoT solution deployment in humanitarian operations within conflict zones are distinct and vary from the difficulties of using IoT in regular warfare, as illustrated in Table 2, Gaps were identified in terms of infrastructure, cybersecurity, power, interoperability, ethics, and socio-political issues. To bridge these gaps, technological and regulatory innovations and engagement strategies that are specific to the local context need to be integrated to make the deployment of IoT sustainable and efficient.

Table 2. Gaps to Solution

Identified Gaps	Proposed Solutions	References	Cross-Check Action
Infrastructure Limitations (Connectivity)	Mesh networks, LPWAN, hybrid connectivity (LoRa, satellite, edge computing)	[3], [4], [33]	Confirmed the papers explicitly discuss infrastructure limitations related to connectivity.
Cybersecurity Risks	End-to-end encryption, blockchain-based verification, AI-driven IDS, decentralized authentication systems	[3], [6], [7], [18]	Confirmed articles explicitly discuss cybersecurity risks in humanitarian aid, particularly in the context of IoT, blockchain, and transparency in humanitarian logistics.
Power Supply Disruptions	Solar panels, generators, decentralized energy management systems	[4], [7]	Confirmed the articles mention power-related challenges in the context of IoT implementation.
Location Privacy Risks	Privacy-preserving techniques (mix-zones, differential privacy), decentralized data management frameworks	[16], [55]	Confirmed the articles discuss drone logistics, security, and operational risks, that logically location tracking as an initial adversarial action.
Satellite Limitations (Cost, Bandwidth)	AI-driven network optimization, hybrid connectivity models (mesh, satellite, edge computing)	[13], [14], [15]	Confirmed articles mention and discuss about satellite coverage limitations, connectivity, bandwidth, and cost
Standardization and Interoperability Issues	Standardized protocols, open -source IoT frameworks, blockchain security	[3], [43]	Confirmed articles discusses standardization and interoperability issues in humanitarian logistic and contexts
Ethical and Data Governance Concerns	Ethical regulatory frameworks, secure multi-party computation (SMPC), transparent data governance	[7], [36], [38]	Confirmed articles mention and discuss ethical and data governance issues related to IoT, particularly in the context of privacy, security, and humanitarian logistics.

Technocolonialism and Power Asymmetries	Local capacity-building, culturally sensitive participatory design, equitable data governance	[8], [29], [36]	Confirmed article discusses data control, governance, or security risks in IoT, it can be indirectly linked to concerns about techno-colonialism and power asymmetries
Limited Adoption of Innovations Due to Costs and Knowledge Barriers	Public-private partnerships, targeted capacity-building, clear regulatory frameworks	[10], [36], [50]	Confirmed the articles mention or discuss about financial constraint, technical gaps, public-private partnership, regulatory uncertainty and capacity- building initiatives.
Environmental Sustainability Concerns	Biodegradable sensors, renewable energy solutions, decentralized logistics (UAV-supported warehouses)	[3], [26], [43]	Confirmed articles mention or discuss about environmental sustainability concerns in varying extents.

4.6.1 Infrastructure Limitations (Connectivity)

One of the most serious issues is the instability of the connection in the conflict zones, which limits real-time data transfer and operational control. Traditional centralized networks are unlikely to be feasible due to damaged infrastructure, high deployment costs, and technical limitations. As a result, hybrid connectivity solutions based on mesh networks, Low-Power WideArea Networks (LPWAN), satellite communication, and edge computing are proposed as alternatives with resilient connectivity. These technologies create decentralized and peer-to-peer network architectures that are able to heal themselves and thus remain operational in the environment of damaged infrastructure.

4.6.2 Cybersecurity Risks

The IoT-enabled humanitarian operations are processing sensitive data such as the location of aid convoys, medical supply logistics, and beneficiary information. These datasets are very valuable and are likely to be subjected to cyber threats, which may range from unauthorized access and data manipulation to cyber attacks. To mitigate these risks, there is the need to have robust cybersecurity frameworks that include end-to-end encryption, blockchain-based data verification, AI based Intrusion Detection Systems (IDS), and decentralized authentication mechanisms. Blockchain improves data reliability and immutability, while AI-based IDS helps in constant monitoring of the network for any suspicious activities before they can become an actual threat

4.6.3 Power Supply Disruptions

Having reliable energy sources is very important for the operation of the IoT; however, in conflict zones, there is a serious problem with power supply due to damage to the infrastructure. Many times, power failures affect monitoring systems, data collection, and communication networks, which are a great blow to the efforts made in the humanitarian response. The challenge can be solved by solar panels, portable generators, and decentralized energy management systems as sustainable energy solutions. These alternative energy sources decrease the dependency on gridbased power and improve the robustness of IoT deployments in extended conflict environments.

4.6.4 Location Privacy Risks

Real-time tracking of humanitarian operations increases logistics efficiency but poses serious privacy risks. If location data is intercepted, it could threaten the security of aid workers, beneficiaries, and resource convoys. To balance transparency and security in the operations, mixzones, differential privacy, decentralized data management frameworks, etc., must be integrated. These techniques guarantee that the critical operational data is accessible to the authorized entities without revealing the patterns that could be used by malicious actors to identify specific entities.

4.6.5 Satellite Limitations (Cost and Bandwidth)

Satellite communication is a viable alternative for connectivity in conflict zones but is limited by high costs and bandwidth constraints, for instance, such networks are used in Iraq and Afghanistan. This paper concludes that AI-driven network optimization and hybrid connectivity models are essential for satellites to be efficient. AI-based adaptive routing can make reasonable decisions on how to manage the available bandwidth for high-priority traffic, and the integration of satellite networks with mesh and edge computing can enhance scalability, reduce latency, and improve overall communication efficiency.

4.6.6 Standardization and Interoperability Issues

As a result of the absence of standardized IoT frameworks in humanitarian contexts, the systems are disjointed and have problems with integration. IoT solutions, communication protocols, and data formats hamper real-time information sharing across organizations. To overcome these barriers, standardized protocols, open-source IoT frameworks, and blockchain-based security solutions should be adopted. These measures facilitate interoperability, improve data-sharing efficiency, and build confidence between humanitarian agencies, government bodies, and private sector partners.

4.6.7 Ethical and Data Governance Concerns

Data governance is still a big issue in humanitarian IoT implementations, and issues regarding data ownership, consent, and the proper use of the gathered information are still relevant. These concerns include the risk of data misuse, surveillance, and potential exploitation by external actors; thus, the development of ethical regulatory frameworks, secure multi-party computation (SMPC), and transparent data governance policies are required. SMPC is the method of collaborative data analysis without the exposure of the raw data to ensure that privacy rights are respected while decision-making is based on data.

4.6.8 Technocolonialism and Power Asymmetries

Such humanitarian IoT initiatives are designed by external stakeholders, which leads to issues like power imbalance, digital sovereignty, and technocolonialism. In order to achieve equitable and inclusive technology deployment, local capacity building, culturally sensitive participatory design, and equitable data governance must be prioritized. This is because involving the local communities in the design and implementation of IoT solutions brings in ownership, trust, and sustainability.

4.6.9 Limited Adoption of Innovations Due to Costs and Knowledge Barriers

However, the use of IoT in the humanitarian setting is still limited due to the existing challenges of financial constraints and technical knowledge gaps. Sophisticated IoT infrastructures are often costly and time-consuming to develop and manage, which limits the ability of public and nonprofit organizations to implement and maintain them. Public-private partnerships (PPPs), capacity-building programs, and appropriate regulatory frameworks are vital to bridge this gap. Through collaboration with PPPs, humanitarian organizations can get financial and technical support and scalable solutions compatible with ethical and operational concerns.

4.6.10 Environmental Sustainability Concerns

IoT deployments in humanitarian operations must also consider long-term environmental impacts. The use of biodegradable sensors, renewable energy solutions, and decentralized logistics (such as UAV-supported warehouses) reduces ecological footprints while maintaining operational efficiency. These sustainable technologies enhance resilience and align with broader humanitarian principles of sustainability and responsible resource management.

In summary, the right way to implement IoT solutions in conflict zones is to combine technological strength, cybersecurity, ethical governance, and a localized approach. In this way, IoT can become a game changer in humanitarian operations by enhancing current practices, reducing response times, and improving operational efficiency and overall performance. Future work should also aim to strengthen interoperable frameworks, AI-driven optimizations, and equity of access to IoT innovations. The sustainability and the ethics of the deployment are critical to making sure that IoT technologies are used as forces of humanitarian action and not as digital divide enablers.

5. Ethical Evaluation and Humanitarian Safeguard

The IEEE Ethically Aligned Design (EAD) framework provides ethical foundations for IoT ethics through technical dependability and political self-determination, but the Ethics Canvas offers practical tools to visualize these principles in stakeholder interactions and deployment strategies. The Ethics Canvas originated as a tool to assist researchers and entrepreneurs and policymakers in identifying ethical risks during project design, yet it demonstrates flexibility for humanitarian technology contexts where quick deployment restricts ethical discussion.

The Ethics Canvas helps identify conflict-zone IoT deployment impacts across its defined dimensions which reveals important risks that standard policy reviews might miss but are essential for field operations.

5.1 Overview of Key Ethical Risk

The implementation of IoT technologies within conflict-affected humanitarian areas creates specific ethical challenges that researchers have not fully investigated. The affected areas present distinctive power inequalities together with state authority breakdowns and surveillance dangers and elevated risks for the affected communities. IoT devices including biometric checkpoints and GPS-enabled aid delivery trackers pose accidental threats to individuals because their data exposure could result in harm or stigmatization or retaliation from improper data handling

The ethical issues surpass basic data protection concerns in these specific situations. The fundamental humanitarian principles of neutrality and impartiality and the "do no harm" mandate face direct challenges because devices transmit sensitive data through unsecured networks and because devices are perceived as surveillance tools. The lack of proper consent because of language barriers and power differences and digital knowledge gaps creates a risk that IoT interventions will become forms of technological imposition.

The section recognizes these risks through a dual-framework approach which includes IEEE Ethically Aligned Design (EAD) principles for global human rights and ethical AI norms (Section 5.2) and the Ethics Canvas for operationalizing principles by mapping stakeholder impacts and contextual risks (Section 5.3). The structured method allows humanitarian technologists and decision-makers to build ethical safeguards into IoT system design at both conceptual and field levels.

5.1.1 Overview of Key Ethical Risk

The research uses two separate frameworks which support ethical assessment of IoT in conflict zones: IEEE Ethically Aligned Design (EAD) and Ethics Canvas. The IEEE Ethically Aligned Design (EAD) provides value-based design principles for AI and emerging technologies, but the Ethics Canvas focuses on practical ethical risk assessment and stakeholder analysis during technology development. Table 3 outlines their initial function and their expanded application to humanitarian missions.

Table 3. Ethical Frameworks: General Purpose vs. Humanitarian IoT Relevance

Framework	Original Purpose	Adapted Use in Humanitarian IoT Context
IEEE Ethically Aligned Design (EAD)	Developed by IEEE to guide ethical development of AI and autonomous systems; emphasizes human rights, transparency, and accountability in design and deployment [85].	Provides normative principles to ensure IoT deployments in conflict zones uphold humanitarian values, prevent harm, and protect individual dignity and autonomy.[85], [86]
Ethics Canvas	Created as a design-thinking tool to help teams reflect on ethical risks and stakeholder impact in product/service innovation. [87]	Enables humanitarian actors to map practical risks, including unintended surveillance, unequal access, and device misuse; supports iterative ethical foresight during deployment [86], [87]

The combination of these frameworks establishes a dual-level ethical protection system which uses IEEE EAD to base the system on worldwide ethical standards and the Ethics Canvas to apply these principles to operational field-based design choices.

5.2 Ethical Principles – Applying IEEE EAD

The previous sections provided general information about data protection and consent but a systematic ethical evaluation must be conducted to ensure IoT deployments follow worldwide recognized standards. The IEEE Ethically Aligned Design (EAD) framework provides a solid basis for ensuring that emerging technologies including IoT systems promote human dignity and well-being and social justice. The importance of EAD principles becomes more significant in humanitarian situations because affected populations usually do not possess control or decision-making abilities or digital understanding.

The following Table 4 demonstrates how the fundamental IEEE EAD principles should be implemented during IoT-enabled humanitarian interventions in conflict zones. This framework functions as both a design-time evaluation system and an accountability framework for postdeployment assessment:

Table 4. Ethical Evaluation of Humanitarian IoT Using IEEE EAD Principles

IEEE EAD Principle	Application in Humanitarian IoT Deployments
Human Rights	The devices need to always protect privacy and dignity and autonomy of users. The collection of data needs to be limited to essential purposes while avoiding any form of coercion.
Human Well- being	The technology needs to provide direct support for population safety and health needs and mobility requirements instead of serving military purposes or donor monitoring needs.
Transparency & Explainability	The beneficiaries need to receive clear information about device functions and deployment reasons as well as data usage procedures. Visual guides and localized communication are essential.
Accountability	The responsible party must be identified by aid agencies to handle cases of device malfunctioning and data breaches and unintended adverse effects. The organization needs to provide third-party audit capabilities and grievance mechanisms.
Data Agency and Consent	People must have the freedom to choose participation or non-participation without facing any adverse consequences. The consent process needs to be both fully explained to participants and easily reversible and properly recorded regardless of the communication method used in areas with limited literacy skills.

IEEE EAD implementation goes beyond supporting abstract values because it establishes technical innovation on humanitarian principles of neutrality and impartiality and accountability. The ethical design of IoT systems becomes possible through field insights and local partnerships which ensure ethical standards beyond regulatory requirements.

5.3 Operationalizing Ethics – Insight from the Ethics Canvas

The IEEE Ethically Aligned Design (EAD) framework offers principled guidance but ethical considerations for humanitarian IoT deployment need to be practical and contextual and iterative. The Ethics Canvas functions as a visual thinking tool which supports ethical responsible innovation by enabling project teams to identify real-world impacts and hidden stakeholders and unintended consequences throughout a technology's life cycle.

The process of making ethical decisions takes place without formal procedures and under urgent conditions in humanitarian conflict zones where operational demands are extreme. The Ethics Canvas enables structured judgment through formalization as demonstrated in Table 5 by asking essential questions about potential harm to people and excluded stakeholders and possible misuse in this environment. The Canvas improves foresight when applied at an early stage and strengthens accountability through post-deployment reviews.

Table 5. Applying the Ethics Canvas to Humanitarian IoT Deployment

Canvas Component	Application in Conflict-Affected Humanitarian Contexts
Stakeholders	Identify both primary (beneficiaries, field workers) and secondary stakeholders (militias, local authorities displaced groups).
Impacts (Positive & Negative)	Assess the intended advantages (faster aid, better targeting) and possible negative consequences (surveillance, stigma, fear, targeting).
Power & Inequality	Analyze how the intervention strengthens dependency or ignores local knowledge systems.
Understanding & Trust	Users need to understand device functions and purposes so implement co-design to combat misperceptions.
Misuse Scenarios	The forecasted risks include device confiscation and third-party data abuse and military intelligence collection through dual-use of devices.
Mitigation Measures	Create culturally suitable visual consent tools and establish default anonymization features and procedures for device removal when devices become compromised.

IEEE EAD establishes ethical integrity while the Ethics Canvas provides tools to identify ethical blind spots in actual humanitarian operations. The dual-framework method provides moral depth and design pragmatism which improves IoT governance in high-stakes conflict environments.

6. Conclusion and Actionable Roadmap

The thematic review demonstrates how Internet of Things (IoT) technologies can revolutionize humanitarian aid delivery in conflict zones. IoT technology provides scalable solutions to operational challenges through its asset tracking and environmental sensing capabilities and predictive analytics features. The review reveals essential gaps which need resolution to achieve responsible and effective deployment.

Future research needs to develop standard operating procedures (SOPs) and interoperable frameworks which will reduce integration barriers between organizational silos. Real-time coordination and decision-making will significantly benefit from shared protocols and interoperable data architecture. Cybersecurity needs to be the highest priority because decentralized authentication systems combined with end-to-end encryption and blockchain-based data registries will protect trust and availability and maintain data integrity in unstable zones.

The ethical deployment of IoT systems requires special attention in conflict areas because power inequalities and digital knowledge gaps and coercive conditions increase the chances of exploitation. Every stage of operations needs to protect data sovereignty together with informed consent and meaningful community participation. Sustainability demands a long-term approach which directs investments toward green energy systems and biodegradable sensors and lowimpact digital logistics that meet environmental and humanitarian requirements.

The success of operations depends on inclusive stakeholder engagement through co-design of culturally adapted systems and public–private partnerships (PPPs) and local technical actor empowerment. The implementation of ethical frameworks such as IEEE Ethically Aligned Design and Ethics Canvas provides both moral protection and practical direction to establish trustworthy and legitimate IoT interventions.

The proposed roadmap, outlined in Table 6, serves as a path to advance past theoretical discussions by establishing future action directions. The strategy emerges from field deployments and stakeholder consultations to provide a tiered approach for ethically aligned and technically feasible and context-aware IoT adoption in humanitarian conflict settings.

Table 6. Actionable Roadmap for IoT in Humanitarian Conflict Response

Timeline	Strategic Recommendation	Key Stakeholders
2025	Pilot LoRaWAN–Satellite hybrid connectivity kits in insecure environments to overcome network blackouts.	ICRC, MSF, UN OCHA
2026	Develop and disseminate a standardized Data Ethics Toolkit tailored for humanitarian IoT.	IEEE, IFRC, humanitarian ethics boards
2027	Scale secure, consent-based IoT deployments in collaboration with local communities.	Local NGOs, Red Crescent, civil society
2028+	Establish global guidelines for humanitarian-grade IoT infrastructure, with independent auditing mechanisms.	UNOCHA, ISO, SphereProject, donors

This roadmap bridges the gap between vision and execution ensuring that the future of IoT in humanitarian operations is not only innovative, but also inclusive, ethical, and resilient.

References

[1] J. Dugdale, M. T. Moghaddam, and H. Muccini. “IoT4Emergency”. In: *ACM SIGSOFT Software Engineering Notes* 46.1 (Jan. 2021), pp. 33–36. DOI: 10.1145/3437479.3437489.

[2] S. K. Ahmed et al. “The role of digital health in revolutionizing healthcare delivery and improving health outcomes in conflict zones”. In: *Digit Health* 9 (2023). DOI: 10.1177/20552076231218158.

[3] A. Fekete et al. “Bridging Gaps in Minimum Humanitarian Standards and Shelter Planning by Critical Infrastructures”. In: *Sustainability* (2021). DOI: 10.3390/SU13020849.

[4] I. Idris. *Humanitarian Digital Transfers in Challenging Contexts*. 2024. DOI: 10.19088/k4dd.2024.033.

[5] K. Stanski. “Humanitarian Health Responses in Urban Conflict Zones”. In: *Daedalus* 152 (2023), pp. 70–82. DOI: 10.1162/daed_a_01993.

[6] M. Khan et al. “Integration of Internet-of-Things With Blockchain Technology to Enhance Humanitarian Logistics Performance”. In: *IEEE Access* 9 (2021), pp. 25422–25436. DOI: 10.1109/ACCESS.2021.3054771.

[7] M. Khan et al. “A Model for Understanding the Mediating Association of Transparency between Emerging Technologies and Humanitarian Logistics Sustainability”. In: *Sustainability* (2022). DOI: 10.3390/su14116917.

[8] A. K. Junejo, M. Breza, and J. McCann. “Threat Modeling for Communication Security of IoT-Enabled Digital Logistics”. In: *Sensors (Basel)* 23 (2023). DOI: 10.3390/s23239500.

[9] U. A. Usmani, A. Happonen, and J. Watada. “Secure Integration of ioT-Enabled Sensors and Technologies: Engineering Applications for Humanitarian Impact”. In: *2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*. 2023, pp. 1–10. DOI: 10.1109/HORA58378.2023.10156740.

[10] R. Bail et al. “Internet of things in disaster management: technologies and uses”. In: *Environmental Hazards* 20 (2021), pp. 493–513. DOI: 10.1080/17477891.2020.1867493.

[11] U. O. Paul-Chima et al. “Harnessing technology for infectious disease response in conflict zones: Challenges, innovations, and policy implications”. In: *Medicine* 103 (2024). DOI: 10.1097/MD.0000000000038834.

[12] W. Gutjahr et al. “Innovative approaches in humanitarian operations”. In: *Or Spectrum* 42 (2020), pp. 585–589. DOI: 10.1007/s00291-020-00598-6.

[13] M. Centenaro et al. “A Survey on Technologies, Standards and Open Challenges in Satellite IoT”. In: *IEEE Communications Surveys & Tutorials* 23 (2021), pp. 1693–1720. DOI: 10.1109/COMST.2021.3078433.

[14] R. Dwivedi, D. Mehrotra, and S. Chandra. “Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review”. In: *J Oral Biol Craniofac Res* 12.2 (Mar. 2022), pp. 302–318. DOI: 10.1016/j.jobcr.2021.11.010.

[15] A. A. Pise et al. “Enabling Artificial Intelligence of Things (AIoT) Healthcare Architectures and Listing Security Issues”. In: *Comput Intell Neurosci* 2022 (Aug. 2022), pp. 1–14. DOI: 10.1155/2022/8421434.

[16] H. Jeong et al. “The humanitarian flying warehouse”. In: *Transportation Research Part E: Logistics and Transportation Review* 136 (2020), p. 101901. DOI: 10.1016/j.tre.2020.101901.

[17] A. Rejeb et al. “Drones for supply chain management and logistics: a review and research agenda”. In: *International Journal of Logistics Research and Applications* 26 (2021), pp. 708–731. DOI: 10.1080/13675567.2021.1981273.

[18] D.-H. Tran et al. “UAV Relay-Assisted Emergency Communications in IoT Networks: Resource Allocation and Trajectory Optimization”. In: *IEEE Transactions on Wireless Communications* 21 (2020), pp. 1621–1637. DOI: 10.1109/TWC.2021.3105821.

[19] A. Balasundaram et al. “Internet of Things (IoT)-Based Smart Healthcare System for Efficient Diagnostics of Health Parameters of Patients in Emergency Care”. In: *IEEE Internet of Things Journal* 10 (2023), pp. 18563–18570. DOI: 10.1109/JIOT.2023.3246065.

[20] C. Egger. “The politics and spaces of public-private partnerships in humanitarian tech innovations”. In: *Environment and Planning C: Politics and Space* (2023). DOI: 10.1177/23996544231206822.

[21] S. Asaithambi et al. “Blockchain-Assisted Hierarchical Attribute-Based Encryption Scheme for Secure Information Sharing in Industrial Internet of Things”. In: *IEEE Access* 12 (2024), pp. 12586–12601. DOI: 10.1109/ACCESS.2024.3354846.

[22] R. Dubey et al. “Blockchain technology for enhancing swift-trust, collaboration and resilience within a humanitarian supply chain setting”. In: *International Journal of Production Research* 58 (2020), pp. 3381–3398. DOI: 10.1080/00207543.2020.1722860.

[23] H. D. Zubaydi, P. Varga, and S. Molnár. “Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review”. In: *Sensors (Basel)* 23 (2023). DOI: 10.3390/s23020788.

[24] P. Sun et al. “A Survey of IoT Privacy Security: Architecture, Technology, Challenges, and Trends”. In: *IEEE Internet of Things Journal* 11 (2024), pp. 34567–34591. DOI: 10.1109/JIOT.2024.3372518.

[25] R. Ahmad and I. Alsmadi. “Machine learning approaches to IoT security: A systematic literature review”. In: *Internet of Things* 14 (2021), p. 100365. DOI: 10.1016/J.IOT.2021.100365.

[26] E. Cadet et al. “AI-powered threat detection in surveillance systems: A real-time data processing framework”. In: *Open Access Research Journal of Engineering and Technology* (2024). DOI: 10.53022/oarjet.2024.7.2.0057.

[27] M. Pradhan. “Federation Based on MQTT for Urban Humanitarian Assistance and Disaster Recovery Operations”. In: *IEEE Communications Magazine* 59 (2021), pp. 43–49. DOI: 10.1109/MCOM.001.2000937.

[28] Guido Álvarez et al. “Uplink transmission policies for LoRa-based direct-to-satellite IoT”. In: *IEEE Access* 10 (2022), pp. 72687–72701.

[29] F. Kagai et al. “Rapidly Deployable Satellite-Based Emergency Communications Infrastructure”. In: *IEEE Access* 12 (2024), pp. 139368–139410. DOI: 10.1109/ACCESS.2024.3465512.

[30] Z. Qin et al. “Multi-Agent Reinforcement Learning Aided Computation Offloading in Aerial Computing for the Internet-of-Things”. In: *IEEE Transactions on Services Computing* 16 (2023), pp. 1976–1986. DOI: 10.1109/TSC.2022.3190562.

[31] S. E. Henriksen. “Humanitarian hacking: Merging refugee aid and digital capitalism”. In: *Journal of Refugee Studies* (2024). DOI: 10.1093/jrs/feae017.

[32] K. Weitzberg et al. “Between surveillance and recognition: Rethinking digital identity in aid”. In: *Big Data Society* 8 (2021). DOI: 10.1177/20539517211006744.

[33] V. Lanfranchi, N. Noori, and T. Sirbu. *GPS-based solution for tracking and protecting humanitarians in conflict zones.* [Online]. Available: https://consensus.app/papers/gpsbased-solution-for-tracking-and-protecting-lanfranchi-noori/df4758c7cefb59c287253d9a6be5baa7/. 2018.

[34] M. Madianou. “Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises”. In: *Social Media + Society* 5 (2019). DOI: 10.1177/2056305119863146.

[35] I. Sahebi, B. Masoomi, and S. Ghorbani. “Expert oriented approach for analyzing the blockchain adoption barriers in humanitarian supply chain”. In: *Technology in Society* 63 (2020), p. 101427. DOI: 10.1016/j.techsoc.2020.101427.

[36] E. Luvison et al. *A Low-Cost Privacy-Preserving Digital Wallet for Humanitarian Aid Distribution.* [Online]. Available: https://consensus.app/papers/a-lowcost-privacypreserving-digital-wallet-for-luvison-chatel/2b531ce40d565aa784b3f859192aabd5/. 2024.

[37] G. Pinto et al. “A Systematic Review on Privacy-Aware IoT Personal Data Stores”. In: *Sensors (Basel)* 24 (2024). DOI: 10.3390/s24072197.

[38] K. Sollins. “IoT Big Data Security and Privacy Versus Innovation”. In: *IEEE Internet of Things Journal* 6 (2019), pp. 1628–1635. DOI: 10.1109/JIOT.2019.2898113.

[39] C. L’Hermitte and N. Nair. “A blockchain-enabled framework for sharing logistics resources in emergency operations”. In: *Disasters* (2020). DOI: 10.1111/disa.12436.

[40] C. Wang et al. “Research on emergency logistics information traceability model and resource optimization allocation strategies based on consortium blockchain”. In: *PLoS ONE* 19 (2024). DOI: 10.1371/journal.pone.0303143.

[41] I. Butun and I. Mahgoub. “Expandable Mix-Zones as a Deception Technique for Providing Location Privacy on Internet-of-Battlefield Things (IoBT) Deployments”. In: *IEEE Access* 12 (2024), pp. 149647–149661. DOI: 10.1109/ACCESS.2024.3461609.

[42] K. Kanciak, K. Wrona, and M. Jarosz. “Secure Onboarding and Key Management in Federated IoT Environments”. In: *2022 17th Conference on Computer Science and Intelligence Systems (FedCSIS)*. 2022, pp. 627–634. DOI: 10.15439/2022F173.

[43] M. Hunt et al. “Ethics of emergent information and communication technology applications in humanitarian medical assistance”. In: *International Health* 8.4 (2016), pp. 239–245. DOI: 10.1093/inthealth/ihw028.

[44] O. Rodríguez-Espíndola et al. “The potential of emergent disruptive technologies for humanitarian supply chains: the integration of blockchain, Artificial Intelligence and 3D printing”. In: *International Journal of Production Research* 58 (2020), pp. 4610–4630. DOI: 10.1080/00207543.2020.1761565.

[45] A. Martin et al. “Digitisation and Sovereignty in Humanitarian Space: Technologies, Territories and Tensions”. In: *Geopolitics* 28 (2022), pp. 1362–1397. DOI: 10.1080/14650045.2022.2047468.

[46] R. K. Singh. “Leveraging technology in humanitarian supply chains: impacts on collaboration, agility and sustainable outcomes”. In: *Journal of Humanitarian Logistics and Supply Chain Management* (2024). DOI: 10.1108/jhlscm-05-2024-0063.

[47] S. Siddiqui et al. “Toward Software-Defined Networking-Based IoT Frameworks: A Systematic Literature Review, Taxonomy, Open Challenges and Prospects”. In: *IEEE Access* 10 (2022), pp. 70850–70901. DOI: 10.1109/access.2022.3188311.

[48] A. Holiatkin and A. Moshynska. “Expanding the functionality of IoT devices in conditions of emergency situations”. In: *Collection “Information Technology and Security”* (2023). DOI: 10.20535/2411-1031.2023.11.2.293493.

[49] A. Karale. “The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws”. In: *Internet of Things* 15 (2021), p. 100420. DOI: 10.1016/J.IOT.2021.100420.

[50] A. Khalid et al. “Supporting the use of research evidence in decision-making in crisis zones in low- and middle-income countries: a critical interpretive synthesis”. In: *Health Research Policy and Systems* 18 (2020). DOI: 10.1186/s12961-020-0530-2.

[51] T. Tabaklar et al. “Exploring the microfoundations of dynamic capabilities for social innovation in a humanitarian aid supply network setting”. In: *Industrial Marketing Management* (2021). DOI: 10.1016/J.INDMARMAN.2021.04.012.

[52] R. Dubey, A. Gunasekaran, and C. Foropon. “Improving information alignment and coordination in humanitarian supply chain through blockchain technology”. In: *Journal of Enterprise Information Management* 37 (2022), pp. 805–827. DOI: 10.1108/jeim-07-2022-0251.

[53] M. Adil et al. “UAV-Assisted IoT Applications, QoS Requirements and Challenges with Future Research Directions”. In: *ACM Computing Surveys* 56 (2024), pp. 1–35. DOI: 10.1145/3657287.

[54] M. Ren et al. “Collaborative Data Acquisition for UAV-Aided IoT Based on Time-Balancing Scheduling”. In: *IEEE Internet of Things Journal* 11 (2024), pp. 13660–13676. DOI: 10.1109/JIOT.2023.3339136.

[55] B. Yang et al. “Unmanned Aerial Vehicle Assisted Post-Disaster Communication Coverage Optimization Based on Internet of Things Big Data Analysis”. In: *Sensors (Basel)* 23 (2023). DOI: 10.3390/s23156795.

[56] G. Kabra et al. “Barriers to information and digital technology adoption in humanitarian supply chain management: a fuzzy AHP approach”. In: *Journal of Enterprise Information Management* 36 (2023), pp. 505–527. DOI: 10.1108/jeim-10-2021-0456.

[57] N. Wang, M. Christen, and M. Hunt. “Ethical Considerations Associated with ‘Humanitarian Drones’: A Scoping Literature Review”. In: *Science and Engineering Ethics* 27 (2021). DOI: 10.1007/s11948-021-00327-4.

[58] H. Baharmand, A. Maghsoudi, and G. Coppi. “Exploring the application of blockchain to humanitarian supply chains: insights from Humanitarian Supply Blockchain pilot project”. In: *International Journal of Operations Production Management* (2021). DOI: 10.1108/IJOPM-12-2020-0884.

[59] R. R. Raj. “Emergency Communication System for Hills and Forest Region Using IOT”. In: *International Journal of Innovative Research in Information Security* (2024). DOI: 10.26562/ijiris.2024.v1003.13.

[60] A. Buzachis et al. “Infrastructureless IoT-as-a-Service for Public Safety and Disaster Response”. In: *2019 7th International Conference on Future Internet of Things and Cloud (FiCloud)*. 2019, pp. 133–140. DOI: 10.1109/FiCloud.2019.00026.

[61] K. Haseeb et al. “RTS: A Robust and Trusted Scheme for IoT-Based Mobile Wireless Mesh Networks”. In: *IEEE Access* 8 (2020), pp. 68379–68390. DOI: 10.1109/ACCESS.2020.2985851.

[62] W. D. Paredes et al. “LoRa Technology in Flying Ad Hoc Networks: A Survey of Challenges and Open Issues”. In: *Sensors (Basel)* 23 (2023). DOI: 10.3390/s23052403.

[63] I. Zhou et al. “Secure Multi-Party Computation for Machine Learning: A Survey”. In: *IEEE Access* 12 (2024), pp. 53881–53899. DOI: 10.1109/ACCESS.2024.3388992.

[64] A. P. Kalapaaking, I. Khalil, and X. Yi. “Blockchain-Based Federated Learning With SMPC Model Verification Against Poisoning Attack for Healthcare Systems”. In: *IEEE Transactions on Emerging Topics in Computing* 12 (2023), pp. 269–280. DOI: 10.1109/TETC.2023.3268186.

[65] C. Lupascu, A. Lupascu, and I. Bica. “DLT Based Authentication Framework for Industrial IoT Devices”. In: *Sensors (Basel)* 20 (2020). DOI: 10.3390/s20092621.

[66] A. Hineman and M. Blaum. “A Modified Shamir Secret Sharing Scheme With Efficient Encoding”. In: *IEEE Communications Letters* 26 (2022), pp. 758–762. DOI: 10.1109/lcomm.2022.3144375.

[67] B. Alaya, L. Laouamer, and N. Msilini. “Homomorphic encryption systems statement: Trends and challenges”. In: *Computer Science Review* 36 (2020), p. 100235. DOI: 10.1016/j.cosrev.2020.100235.

[68] A. Al-Fuqaha et al. “Toward better horizontal integration among IoT services”. In: *IEEE Communications Magazine* 53 (2015), pp. 72–79. DOI: 10.1109/MCOM.2015.7263375.

[69] S. Dejean. *IoT Helps U.N. Refugee Program Track Water Volume, Safety - RFID JOURNAL*. Accessed: May 06, 2025. 2025. URL: https://www.rfidjournal.com/news/iot-helps-u-n-refugee-program-track-water-volumesafety/154112/.

[70] United Nations Security Council. *Situation in Abyei - Report of the Secretary-General (S/2022/316)*. Accessed: May 07, 2025. 2025. URL: https://reliefweb.int/report/sudan/situation-abyei-report-secretary-general-s2022316-enar.

[71] MSF-UK. *Innovation: Four ground-breaking projects that are changing the way MSF works*. Accessed: May 06, 2025. 2025. URL: https://msf.org.uk/article/innovation-four-ground-breaking-projects-are-changing-waymsf-works?page=select_amount.

[72] N. Doty. *A Digital Red Cross: Keeping Humanitarian Aid Safe from Cyberattack*. Accessed: May 06, 2025. 2025. URL: https://cdt.org/insights/a-digital-red-cross-keeping-humanitarian-aid-safe-fromcyberattack/.

[73] A. M. Fejerskov, M.-L. Clausen, and S. Seddiq. *Risks of technology use in humanitarian settings: Avoiding harm, delivering impact*. Accessed: May 06, 2025. 2025. URL: https://www.diis.dk/en/research/risks-of-technology-use-inhumanitarian-settings-avoiding-harm-delivering-impact.

[74] P. Veillette. *The Serious Threat Of GPS Spoofing: An Analysis*. Accessed: May 06, 2025. 2025. URL: https://aviationweek.com/business-aviation/safety-ops-regulation/serious-threat-gpsspoofing-analysis.

[75] Human Rights Watch. *Gaza: Israeli Military’s Digital Tools Risk Civilian Harm*. Accessed: May 06, 2025. 2024. URL: https://www.hrw.org/news/2024/09/10/gaza-israeli-militarys-digital-tools-risk-civilianharm.

[76] Radio Tamazuj. *UN Commission: Targeting of Old Fangak MSF Hospital, a war crime*. Accessed: May 06, 2025. 2025. URL: https://www.radiotamazuj.org/en/news/article/un-commission-targeting-of-old-fangakmsf-hospital-a-war-crime.

[77] J. Amstrong. *Changes-in-medical-practice-in-Syria*. Accessed: May 07, 2025. 2016. URL: https://arhp.msf.es/wp-content/uploads/2023/07/Changes-inmedical-practice-in-Syria.pdf.

[78] UNHCR. *Digital Access, Inclusion and Participation Connecting with Confidence Literature Review*. Accessed: May 06, 2025. 2020. URL: https://www.unhcr.org/innovation/wp-content/uploads/2020/03/Connecting-withconfidence-LitRev-Web.pdf.

[79] UNDSS. *Three Years of War: How UNDSS Keeps Humanitarian Aid Moving in Ukraine's War Zone*. Accessed: May 06, 2025. 2025. URL: https://www.un.org/safety-and-security/en/article/three-years-warhow-undss-keeps-humanitarian-aid-moving-ukraines-war-zone.

[80] L. Brogaard. "Innovative outcomes in public-private innovation partnerships: a systematic review of empirical evidence and current challenges". In: *Public Management Review* 23 (2021), pp. 135–157. DOI: 10.1080/14719037.2019.1668473.

[81] J. Burton. "'Doing no harm' in the digital age: What the digitalization of cash means for humanitarian action". In: (2020). DOI: 10.1017/S1816383120000491.

[82] Inter-Agency Standing Committee (IASC). *Operational Guidance: Data Responsibility in Humanitarian Action*. Accessed: May 07, 2025. 2021. URL: https://interagencystandingcommittee.org/sites/default/files/migrated/2021-02/IASC%20Operational%20Guidance%20on%20Data%20Responsibility%20in%20Humanitarian%20Action-%20February%202021.pdf.

[83] SWOT. *Safe Water Optimization Tool*. Accessed: May 07, 2025. 2025. URL: https://www.safeh2o.app/our-story.html.

[84] OCHA. *Guidance Note Series: Data Responsibility In Humanitarian Action*. Accessed: May 07, 2025. 2025. URL: https://www.unocha.org/publications/report/world/centre-humanitarian-data-guidance-note-series-data-responsibility-humanitarian-action-6.

[85] IEEE. *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems, First Edition*. Accessed: May 07, 2025. 2019. URL: https://ieeexplore.ieee.org/document/9398613.

[86] S. Viswanathan. *Designing frameworks for the ethical use of technology in humanitarian programmes - UKHIH*. Accessed: May 07, 2025. 2025. URL: https://www.ukhih.org/news/designing-frameworks-for-the-ethical-use-of-technology-in-humanitarian-programmes/.

[87] C. Mcginn. *Informing the Design of HRI Systems through Use of the Ethics Canvas*. Accessed: May 07, 2025. 2025. URL: https://www.armydistaff.org/wp-content/uploads/2020/09/Applying-Ethical-Canvas-For-HRI-Applications.pdf.