DEVOTION
Journal of Research and Community Service
Volume 6, Number 4, April 2025
e-ISSN: 2797-6068 and p-ISSN: 2777-0915

Transforming Conflict Response with IoT: Innovations, Challenges, and Ethical Considerations in Humanitarian Aid Delivery

Budi Dhaju Parmadia, Kallamullah Ramlib
Universitas Indonesia, Indonesia
Email: budi.dhaju31@ui.ac.ida, Kalamullah.ramli@ui.ac.idb

KEYWORDS
Humanitarian IoT, Conflict Zones, Cybersecurity, Blockchain, Ethical Data Governance

ABSTRACT
The integration of Internet of Things (IoT) technologies in humanitarian aid holds transformative potential for conflict zones but faces critical challenges, including infrastructure degradation, cybersecurity risks, and ethical dilemmas. This study systematically reviews 75 peer-reviewed sources (2019–2024) using the PRISMA methodology to analyze IoT adoption barriers and innovations. Findings reveal that decentralized architectures (e.g., blockchain, mesh networks) and AI-driven security (e.g., intrusion detection) can mitigate infrastructure and cyber vulnerabilities, while participatory design and ethical frameworks address techno-colonialism and data sovereignty concerns. The research contributes actionable recommendations for scalable, culturally sensitive IoT deployments, emphasizing hybrid connectivity (LoRa, satellite) and sustainable practices (biodegradable sensors). Implications include fostering multi-stakeholder collaboration, standardized protocols, and longitudinal field testing to ensure resilience and equity in humanitarian operations. This study bridges theoretical and practical gaps, offering a holistic roadmap for ethically grounded IoT solutions in high-risk environments.

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, improving 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 (Dugdale J., 2021).

These obstacles must be addressed to realize the maximum potential of IoT 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 simultaneously addresses infrastructural, security, and ethical dimensions.

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 most significant constraints (Ahmed, Chandran, Islam, & Dhama, 2023; Fekete, A., 2021; Idris, 2024). Infrastructure Limitations (9/10) are the worst, based on damaged communication networks, unstable power grids, and limited hardware availability in conflict zones. Cybersecurity Vulnerabilities (9/10) are a critical threat due to cyberattacks, unauthorized access, and data breaches that can compromise sensitive information and halt aid logistics (Junejo A. K., 2023). 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 (Bail Kovaleski, Da

Silva, Pagani, & Chiroli, 2021). 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.

Many conflict-affected regions face degraded power grids, communication networks, and transportation systems that hinder IoT deployment (Ahmed et al., 2023)Paul-Chima et al., 2024), with unreliable infrastructure challenging data flow and operational efficiency (Ahmed et al., 2023; Dugdale J., 2021). While IoT systems require uninterrupted data exchange for monitoring, security threats, and population movements (Ahmed et al., 2023), unstable connectivity disrupts device-command center communication, impairing real-time decisions and delaying interventions (Centenaro M., 2021; Dugdale J., 2021). High-risk settings also expose IoT to cyberattacks and unauthorized access, necessitating encryption, secure protocols, and robust architectures to protect sensitive data like medical records and convoy locations (Dugdale J., 2021)Solutions to enhance security and system resilience include end-to-end encryption (Usmani et al., 2023), blockchain verification, and AI-driven intrusion detection.

Many conflict-affected regions face degraded power grids, communication networks, and transportation systems that hinder IoT deployment (Ahmed et al., 2023) Paul-Chima et al., 2024), with unreliable infrastructure challenging data flow and operational efficiency (Ahmed et al., 2023; Dugdale J., 2021). While IoT systems require uninterrupted data exchange for monitoring, security threats, and population movements(Ahmed et al., 2023) Paul-Chima et al., 2024; Usmani et al., 2023), unstable connectivity disrupts device-command center communication, impairing real-time decisions and delaying interventions (Centenaro M., 2021; Dugdale J., 2021) . High-risk settings also expose IoT to cyberattacks and unauthorized access, necessitating encryption, secure protocols, and robust architectures to protect sensitive data like medical records and convoy locations (Dwivedi R., 2022). Solutions include end-to-end encryption, blockchain verification, and AI-driven intrusion detection to enhance security and system resilience.

This article aims to analyze the key weaknesses and deficiencies of existing IoT solutions for humanitarian aid, assess emerging innovations for future IoT development, and propose best practices for building sustainable, scalable, and ethically governed IoT systems in humanitarian missions to enhance crisis response effectiveness. This thematic review systematically examines recent literature to provide a holistic understanding of IoT implementation challenges and solutions, with a focus on ethical governance and socio-cultural factors. The article aims to analyze key weaknesses in existing IoT solutions for humanitarian aid, assess emerging innovations for future IoT development, and recommend best practices for sustainable and scalable IoT systems in humanitarian missions.

This study distinguishes itself by offering the first integrated thematic review of IoT implementation in humanitarian aid, simultaneously addressing infrastructural, security, and ethical challenges—a gap in existing literature that often treats these issues in isolation (Ahmed et al., 2023; Egger, 2023). It introduces novel frameworks combining decentralized IoT architectures, blockchain-secured networks, and AI-driven analytics to enhance operational resilience while prioritizing ethical governance and community-centric design. Unlike prior works, this research critically evaluates technocolonialism and power asymmetries in IoT deployments, proposing participatory models to ensure equitable data ownership and local agency (Egger, 2023). Additionally, it advances sustainable solutions like biodegradable sensors and hybrid connectivity (LoRa, mesh networks) tailored for conflict zones, bridging gaps in scalability and environmental impact.

METHOD RESEARCH

This thematic review follows a systematic approach of PRISMA (Figure 2-1) to synthesize critically the 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 peer-reviewed 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 synthesis. Some of the most heavily cited works are blockchain-enhanced IoT security studies (Alvarez, Fraire, Hassan, Céspedes, & Pesch, 2022; Gunasekaran A. Bryde D. Dwivedi Y. K. &. Papadopoulos T. Dubey R., 2020) Khan et al., 2021; Zubaydi et al., 2023), AI-driven analytics for network optimization and cybersecurity (Ahmad & Alsmadi, I., 2021; Cadet E., 2024; Setiawati & Hermanto, 2023), decentralized communication solutions (Bail Kovaleski et al., 2021)satellite communication and connectivity, and their limitations (Alvarez, Fraire et al., 2022; Kagai F., 2024)ethical and governance frameworks (Henriksen, 2024)- Cultural implications, techno-colonial concerns, privacy-preserving humanitarian digital wallet, transparency, and logistic sustainability. The literature is mainly for 2020-2024; 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.

RESULT AND DISCUSSION

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.

Infrastructure Challenges

The deployment of IoT solutions in conflict zones faces significant infrastructure limitations, including unreliable internet connectivity, security vulnerabilities, and the weaknesses of centralized systems (Bail Kovaleski et al., 2021). Cloud-dependent IoT applications struggle in areas with limited or no connectivity, hindering real-time monitoring of aid distribution, medical supplies, and situational awareness (Bail Kovaleski et al., 2021). Centralized systems exacerbate these issues, making decentralized or hybrid models—leveraging edge computing and blockchain—more viable for improving security and operational resilience in unstable environments (Asaithambi Ravi et al., 2024).

Security risks, such as data interception and unauthorized access, pose critical threats to IoT networks in conflict zones, especially when handling sensitive information like beneficiary locations. Robust measures like encryption, device authentication, and cybersecurity

frameworks are essential to mitigate these risks. Additionally, frequent power outages disrupt IoT functionality, compromising data transmission, system integrity, and emergency response efforts (Bail Kovaleski et al., 2021). Limited access to backup energy sources, such as solar panels, further undermines reliability and exposes systems to cyber threats during power fluctuations (Bail Kovaleski et al., 2021).

While satellite networks offer potential solutions, their high costs, bandwidth constraints, and latency issues limit their effectiveness for real-time IoT applications like medical supply tracking (Kagai F., 2024). Scalability is also hindered by bandwidth restrictions, which cap the number of concurrently operable devices (Alvarez, Fraire et al., 2022). Addressing these challenges requires a holistic approach: hybrid connectivity (combining satellite, mesh networks, and edge computing), energy-efficient technologies, and decentralized architectures to ensure sustainable, secure, and resilient IoT deployments in conflict-affected regions.

Security and Privacy Concerns

The deployment of IoT solutions in conflict zones faces significant security and privacy risks due to unstable infrastructure, sensitive data collection, and inadequate protective measures (Butun I., 2024). These vulnerabilities expose humanitarian operations to cyber threats like data breaches, device manipulation, and unauthorized surveillance, endangering aid workers and vulnerable populations. Unreliable connectivity and weak security protocols further exacerbate risks, leaving IoT systems susceptible to intrusions, data interception, and network shutdowns. Location privacy is another critical concern, as adversaries could exploit tracking data to monitor aid convoys and personnel. Compounding these issues, damaged infrastructure and inconsistent security practices hinder robust cybersecurity implementation, necessitating scalable solutions like decentralized authentication and hardware security modules.

Beyond technical challenges, IoT deployments raise ethical dilemmas regarding data governance, consent, and power imbalances in humanitarian settings (Egger, 2023). The lack of legal frameworks and local participation risks misuse of sensitive data by state or non-state actors, while technocolonialism perpetuates unequal control over digital systems (Henriksen, 2024). Current IoT security frameworks remain inadequate, with weak encryption, outdated authentication, and fragmented standards leaving systems vulnerable (Karale, 2021) Usmani et al., 2023). Addressing these issues requires a holistic approach: standardized security protocols, privacy-enhancing technologies (e.g., differential privacy), and secure-by-design architectures (Egger, 2023)Building cybersecurity resilience through capacity development and regulatory compliance is essential to ensuring that IoT solutions can operate safely and ethically in conflict zones.

Standardization and Interoperability

Global standardization and interoperability of IoT technologies are essential for efficient humanitarian aid delivery in conflict zones, where diverse systems and stakeholders must collaborate seamlessly (Bail Kovaleski et al., 2021). Integrated frameworks combining IoT, blockchain, and open-source standards enhance responsiveness, risk management, and logistical efficiency while fostering transparency and trust in aid distribution (Gunasekaran A. &. Foropon C. Dubey R., 2022). Standardized communication protocols enable real-time coordination among NGOs, governments, and local communities, while complementary technologies like biometric identification, UAVs, and big data analytics further improve reliability when embedded within a cohesive regulatory system (Adil, Jan, Khan, & Farouk, 2024). Open-source IoT standards also ensure adaptability, security, and community empowerment by allowing local actors to manage aid.

Robust guidelines and policies are critical for securing IoT deployments in high-risk environments, ensuring data integrity, and preventing fraud through blockchain-based solutions. Federated IoT ecosystems, supported by standardized security protocols, enhance

device onboarding, access control, and network reliability (Bail Kovaleski et al., 2021). Public-private partnerships (PPPs) play a pivotal role in scaling these technologies ethically, particularly for innovations like digital health platforms and humanitarian flying warehouses (HFWs) (Egger, 2023; Jeong H., 2020). Moving forward, global IoT frameworks must prioritize decentralized security mechanisms, cross-sector regulatory alignment, and interoperable data-sharing systems to sustain ethical, resilient, and effective humanitarian operations in conflict zones (Egger, 2023). These efforts will bolster the credibility and adaptability of aid initiatives while ensuring communities have access to deployable and reusable IoT solutions (Idris, 2024).

Comparative Analysis of Humanitarian Cultural Barriers

Despite IoT's potential to improve humanitarian aid, cultural and social factors pose significant challenges, particularly in conflict zones where technological mistrust and low digital literacy prevail (Ahmed et al., 2023). Local communities often perceive IoT solutions as external impositions rather than empowering tools, reflecting historical power imbalances and concerns about techno-colonialism. Regulatory gaps and knowledge barriers further hinder adoption, as unclear policies and high costs limit the implementation of technologies like blockchain for supply chain transparency (Kabra G., 2023). Addressing these challenges requires community-centered approaches, including capacity-building programs and transparent data practices, to foster trust and align solutions with local norms.

Ethical concerns, particularly data privacy and governance, are critical for responsible IoT deployment in humanitarian contexts. Without precise consent mechanisms and equitable data ownership, vulnerable populations risk further exploitation. Culturally sensitive design is essential to avoid neo-colonial pitfalls, as seen in critiques of biometric systems and drone deliveries that prioritize external agendas over local agency. Successful IoT integration demands participatory frameworks that engage communities in co-designing solutions tailored to regional challenges while ensuring infrastructure resilience and security (Asaithambi Ravi et al., 2024). By prioritizing transparency, inclusivity, and adaptive governance, IoT can enhance humanitarian operations ethically and sustainably in conflict-affected regions.

Innovative Connectivity Solutions

Resilient and decentralized communication systems are critical for IoT-enabled humanitarian operations in conflict zones where traditional infrastructure is compromised (Khan et al., 2021, 2022). Wireless Mesh Networks (WMNs) with self-healing capabilities and multi-hop topologies provide reliable connectivity without fixed infrastructure (Buzachis A., 2019) while LPWAN technologies like LoRa enable long-range, low-power data transmission for remote monitoring. AI-driven optimization further enhances network resilience through dynamic bandwidth allocation and predictive fault detection, with blockchain integration ensuring secure data sharing. Complementary innovations like UAV-based humanitarian flying warehouses bypass ground infrastructure limitations to deliver aid in high-risk areas (Jeong H., 2020).

Advancements in adaptive network architectures and decentralized caching strategies will strengthen disaster preparedness by maintaining data accessibility during outages (Bail Kovaleski et al., 2021). Emerging protocols like SPIDERMAN aim to reduce latency and interference in volatile environments (Bail Kovaleski et al., 2021), while hybrid networks combining LoRa, Bluetooth Mesh, and ANT optimize real-time tracking and supply chain management. Future frameworks must prioritize scalable security, intelligent resource allocation, and real-time adaptability to ensure effective, data-driven humanitarian responses. Together, these technologies form an autonomous, secure communication ecosystem that enhances aid coordination and operational resilience in crisis zones.

Enhanced Security and Privacy Frameworks

Ensuring robust data security and privacy is paramount for humanitarian IoT deployments in conflict zones, where cyber threats and unauthorized access present significant risks. Blockchain technology enhances trust and transparency through decentralized storage, tamper-proof records, and smart contracts, mitigating the risks of data breaches in humanitarian logistics (Baharmand Maghsoudi & Coppi, G., 2021). Complementing this, Attribute-Based Encryption (ABE) enables fine-grained access control for sensitive data like health records and beneficiary identities without relying on centralized authorities. AI-driven Intrusion Detection Systems (IDS) further bolster security by providing real-time threat detection and adaptive responses to evolving cyber risks (Ahmad & Alsmadi, I., 2021; Cadet E., 2024), ensuring compliance with ethical data-use standards.

Secure Multi-Party Computation (SMPC) advances privacy in collaborative humanitarian operations by enabling joint data analysis without exposing raw inputs, critical for identity verification and resource allocation in hostile environments (Kalapaaking A. P., 2023). Techniques like Shamir's Secret Sharing and homomorphic encryption optimize SMPC for low-resource settings (Alaya Laouamer & Msilini, N., 2020; Hineman A., 2022). Blockchain, AI-based IDS, and SMPC form a resilient framework that safeguards data integrity, prevents manipulation, and upholds privacy ethics in conflict zones. Future efforts must prioritize scalable cryptographic protocols, adaptive threat detection, and decentralized architectures to strengthen IoT ecosystems for humanitarian aid, ensuring operational reliability and stakeholder trust in high-risk contexts.

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 directly address the specific challenges highlighted earlier, thus maintaining coherence and showing how IoT-enabled humanitarian aid delivery can become more resilient, efficient, and ethical in conflict-affected environments.

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 delivering assistance (Al-Fuqaha, Guizani, Rayes, & Mohammadi, 2015). The use of different communication protocols, such as CoAP, REST, MQTT, and AMQP, poses a challenge to the ease of use of integration with various IoT platforms, which hampers real-time communication and sharing of information among the humanitarian stakeholders(Al-Fuqaha et al., 2015). 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 (Al-Fuqaha et al., 2015). 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 to improve integration and achieve operational transparency and effective coordination of all humanitarian actions (Al-Fuqaha et al., 2015).

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 real-time information exchange and increase operations' transparency. The use of multi-protocol middleware and open-source gateways reduces the technical complexity of the system (Al-Fuqaha et al., 2015) and thus solves the problems associated with infrastructure limitations in the sense of thematic analysis.

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. Practical implications are an increased risk of cyber-attacks, data manipulation, and privacy violations that may disrupt aid operations and endanger the victims (Egger, 2023). These risks are further worsened by the absence of universal security standards, which leads 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. Humanitarian organizations can use Secure Multi-Party Computation (SMPC) and homomorphic encryption to handle beneficiary data safely, even in hostile environments, as identified previously.

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. Moreover, adequately designed Public Private Partnerships (PPPs) could significantly help to solve the problem, although they must be handled properly to avoid the potential of power imbalances and unethical data management, technological and regulatory issues (Brogaard, 2021)It could play a pivotal role in overcoming technological and regulatory barriers if transparently structured. Yet, these must be managed carefully to avoid power imbalances and ensure ethical, equitable data governance.

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. Techno-colonialism and local sovereignty concerns result in resistance to successfully implementing and adopting new IoT technologies in conflict zones. Practical measures that can be taken to overcome these barriers include digital literacy enhancement through capacity-building activities (Kabra G., 2023), a participatory design that is in harmony with the local community needs (Egger, 2023) and openness in communication In this way, culturally appropriate mechanisms (Egger, 2023) 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.

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. 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. 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.

Emerging Innovations and Practical Implications

New technologies like blockchain and AI-driven analytics are potentially valuable in increasing humanitarian logistics' accountability, transparency, and performance. In practice, blockchain-based frameworks offer a clear record of aid distribution and thus reduce corruption risks and increase operational accountability. AI-based predictive analytics help improve the accuracy of the assessment of humanitarian needs and help people act proactively during a crisis. Nevertheless, the actual usage of these technologies raises ethical issues such as bias in algorithms, privacy of data, and equity. Moreover, using biodegradable IoT sensors and decentralized logistics, including HFW based on UAVs, also faces practical issues of scalability, regulatory compliance, and environmental friendliness. To overcome these implementation barriers, there is a need for well-defined regulatory frameworks, open

collaboration between the stakeholders, and constant ethical supervision to guarantee that the technological interventions are feasible and proportionate to the context.

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

The 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 4-1. 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 1. Gaps to Solution

Identified Gaps	Proposed Solutions	References	Cross-Check Action
Infrastructure Limitations (Connectivity)	Mesh networks, LPWAN, hybrid connectivity (LoRa, satellite, edge computing)	(Fekete A., 2021)	Confirmed that the papers explicitly discuss infrastructure limitations related to connectivity.
Cybersecurity Risks	End-to-end encryption, blockchain-based verification, AI-driven IDS, and decentralized authentication systems	(Balasundaram Routray, S., Prabu, J., Krishnan, P., Malla, P. P., & Maiti, M., 2023)	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, and decentralized energy management systems	(Idris, 2024)	Confirmed that 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	(Jeong H., 2020)	**The articles discussed drone logistics, security, and operational risks, logically locating tracking as an initial adversarial action.**
Satellite Limitations (Cost, Bandwidth)	AI-driven network optimization, hybrid connectivity models (mesh, satellite, edge computing)	(Centenaro M., 2021)	Confirmed articles mention and discuss satellite coverage limitations, connectivity, bandwidth, and cost
Standardization and Interoperability Issues	Standardized protocols, open-source IoT frameworks, and blockchain security	(Fekete A., 2021)	Confirmed articles discuss **standardization and interoperability issues** in humanitarian logistics and contexts
Ethical and Data Governance Concerns	Ethical regulatory frameworks, secure multi-party computation (SMPC), and transparent data governance	(Khan et al., 2022; L'Hermitte & Nair, 2020; Pinto et al., 2024)	Confirmed articles **discuss** ethical and data governance issues related to IoT, particularly in the context of privacy, security, and humanitarian logistics.

Identified Gaps	Proposed Solutions	References	Cross-Check Action
Technocolonialism and Power Asymmetries	Local capacity-building, culturally sensitive participatory design, and equitable data governance	(Junejo A. K., 2023)	Confirmed **article discusses data control, governance, or security risks in IoT,** which 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, and clear regulatory frameworks	(Bail Kovaleski et al., 2021)	The articles mentioned or discussed financial constraints, technical gaps, public-private partnerships, regulatory uncertainty, and capacity-building initiatives.
Environmental Sustainability Concerns	Biodegradable sensors, renewable energy solutions, decentralized logistics (UAV-supported warehouses)	(Fekete A., 2021)	Confirmed articles mention or discuss environmental sustainability concerns to varying extents.

Infrastructure Limitations (Connectivity)

One of the most serious issues is the connection instability 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 Wide-Area 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 can heal themselves and thus remain operational in the environment of damaged infrastructure.

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 valuable and likely to be subjected to cyber threats, ranging from unauthorized access and data manipulation to cyberattacks. To mitigate these risks, robust cybersecurity frameworks are needed, including 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 constantly monitor the network for any suspicious activities before they can become an actual threat.

Power Supply Disruptions

Having reliable energy sources is very important for the operation of the IoT; however, in conflict zones, there is a serious power supply problem due to infrastructure damage. Power failures often affect monitoring systems, data collection, and communication networks, which are a significant blow to the efforts made in the humanitarian response. Solar panels, portable generators, and decentralized energy management systems are sustainable solutions that can solve the challenge. These alternative energy sources decrease the dependency on grid-based power and improve the robustness of IoT deployments in extended conflict environments.

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 operations, mix zones, differential privacy, decentralized data management frameworks, etc., must be integrated. These techniques guarantee that critical operational data is accessible to authorized

entities without revealing patterns that could be used by malicious actors to identify specific entities.

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 managing the bandwidth for high-priority traffic. Integrating satellite networks with mesh and edge computing can enhance scalability, reduce latency, and improve communication efficiency.

Standardization and Interoperability Issues

The absence of standardized IoT frameworks in humanitarian contexts results in disjointed systems and integration problems. 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.

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 is 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.

Technocolonialism and Power Asymmetries

Such humanitarian IoT initiatives are designed by external stakeholders, which leads to issues like power imbalance, digital sovereignty, and techno-colonialism. 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 designing and implementing IoT solutions brings ownership, trust, and sustainability.

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.

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 sustainability principles 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.

CONCLUSION

This thematic review highlights IoT's transformative potential for humanitarian aid in conflict zones while identifying critical gaps in interoperability, security, ethics, and sustainability that must be addressed. Future research should develop context-aware frameworks integrating standardized yet adaptive protocols for coordination, decentralized cybersecurity (e.g., blockchain and AI), and participatory co-design with local communities to ensure cultural appropriateness and data sovereignty. Simultaneously, studies must advance sustainable IoT solutions—like biodegradable sensors and solar-powered networks—and conduct longitudinal field evaluations to assess real-world performance in volatile settings, ensuring scalable deployments that uphold environmental and ethical principles without compromising operational resilience.

REFERENCES

Adil, Song, Jan, H. M., Khan, M. K. He X., & Farouk, A. &. Jin Z. M. (2024). UAV-Assisted IoT Applications, QoS Requirements and Challenges with Future Research Directions. *ACM Computing Surveys*, *56*, 1–35.

Ahmad & Alsmadi, I., R. (2021). A systematic literature review of machine learning approaches to IoT security: Internet *Things*, *14*, 100365.

Ahmed, Hussein, Chandran, S. D., Islam, M. R., & Dhama, K. S. K. (2023). The role of digital health in revolutionizing healthcare delivery and improving health outcomes in conflict zones. *Digital Health*, *9*.

Al-Fuqaha, Khreishah, Guizani, M., Rayes, A., & Mohammadi, M. A. (2015). Toward better horizontal integration among IoT services. *IEEE Communications Magazine*, *53*, 72–79.

Alaya Laouamer, L., & Msilini, N., B. (2020). Homomorphic encryption systems statement: Trends and challenges. *Comput. Sci. Rev.*, *36*, 100235.

Alvarez, Fraire, J., Hassan, K., Céspedes, S., & Pesch, D. G. (2022). Uplink Transmission Policies for LoRa-Based Direct-to-Satellite IoT. *IEEE Access*, *10*, 72687–72701.

Asaithambi Ravi, L., Devarajan, M., Selvalakshmi, A., Almaktoom, A., Almazyad, A., Xiong, G., & Mohamed, A. W. S. (2024). Blockchain-Assisted Hierarchical Attribute-Based Encryption Scheme for Secure Information Sharing in Industrial Internet of Things. *IEEE Access*, *12*, 12586–12601.

Baharmand Maghsoudi, A., & Coppi, G., H. (2021). Exploring the application of blockchain to humanitarian supply chains: insights from Humanitarian Supply Blockchain pilot project. *International Journal of Operations & Production Management*.

Bail Kovaleski, J., Da Silva, V. L., Pagani, R., & Chiroli, D. R. (2021). Internet of things in disaster management: technologies and uses. *Environmental Hazards*, *20*, 493–

513.
Balasundaram Routray, S., Prabu, J., Krishnan, P., Malla, P. P., & Maiti, M., A. (2023). Internet of Things (IoT)-Based Smart Healthcare System for Efficient Diagnostics of Health Parameters of Patients in Emergency Care. *IEEE Internet of Things Journal*, *10*, 18563–18570.
Brogaard, L. (2021). Innovative outcomes in public-private innovation partnerships: a systematic review of empirical evidence and current challenges. *Public Management Review*, *23*, 135–157.
Butun I., &. Mahgoub I. (2024). Expandable Mix-Zones as a Deception Technique for Providing Location Privacy on Internet-of-Battlefield Things (IoBT) Deployments. *IEEE Access*, *12*, 149647–149661.
Buzachis A., Fazio M. Galletta A. Celesti A. &. Villari M. (2019). Infrastructureless IoT-as-a-Service for Public Safety and Disaster Response. *2019 7th International Conference on Future Internet of Things and Cloud (FiCloud)*, 133–140.
Cadet E., Osundare O. S. Ekpobimi H. O. Samira Z. &. Weldegeorgise Y. W. (2024). AI-powered threat detection in surveillance systems: A real-time data processing framework. *Open Access Research Journal of Engineering and Technology*.
Centenaro M., Costa C. Granelli F. Sacchi C. &. Vangelista L. (2021). A Survey on Technologies, Standards and Open Challenges in Satellite IoT. *IEEE Communications Surveys & Tutorials*, *23*, 1693–1720.
Dubey R., Gunasekaran A. &. Foropon C. (2022). Improving information alignment and coordination in humanitarian supply chain through blockchain technology. *J. Enterp. Inf. Manag.*, *37*, 805–827.
Dubey R., Gunasekaran A. Bryde D. Dwivedi Y. K. &. Papadopoulos T. (2020). Blockchain technology for enhancing swift-trust, collaboration and resilience within a humanitarian supply chain setting. *International Journal of Production Research*, *58*, 3381–3398.
Dugdale J., Moghaddam M. T. &. Muccini H. (2021). IoT4Emergency. *ACM SIGSOFT Software Engineering Notes*, *46*(1), 33–36.
Dwivedi R., Mehrotra D. &. Chandra S. (2022). Potential of Internet of Medical Things (IoMT) applications in building an innovative healthcare system: A systematic review. *Journal of Oral Biology and Craniofacial Research*, *12*(2), 302–318.
Egger, C. (2023). The politics and spaces of public-private partnerships in humanitarian tech innovations. *Environment and Planning C: Politics and Space*.
Fekete A., Bross L. Krause S. Neisser F. &. Tzavella K. (2021). Bridging Gaps in Minimum Humanitarian Standards and Shelter Planning by Critical Infrastructures. *Sustainability*.
Henriksen, S. E. (2024). Humanitarian hacking: Merging refugee aid and digital capitalism. *Journal of Refugee Studies*.
Hineman A., &. Blaum M. (2022). A Modified Shamir Secret Sharing Scheme With Efficient Encoding. *IEEE Communications Letters*, *26*, 758–762.
Idris, I. (2024). *Humanitarian Digital Transfers in Challenging Contexts*.
Jeong H., Yu D. Min B. &. Lee S. (2020). The humanitarian flying warehouse. *Transportation Research Part E-Logistics and Transportation Review*, *136*, 101901.
Junejo A. K., Breza M. &. McCann J. (2023). Threat Modeling for Communication Security of IoT-Enabled Digital Logistics. *Sensors (Basel, Switzerland)*, *23*.

Kabra G., Anbanandam R. Jain V. &. Akhtar P. (2023). Barriers to information and digital technology adoption in humanitarian supply chain management: a fuzzy AHP approach. *J. Enterp. Inf. Manag.*, *36*, 505–527.
Kagai F., Branch P. But J. Allen R. &. Rice M. (2024). Rapidly Deployable Satellite-Based Emergency Communications Infrastructure. *IEEE Access*, *12*, 139368–139410.
Kalapaaking A. P., Khalil I. &. Yi X. (2023). Blockchain-Based Federated Learning With SMPC Model Verification Against Poisoning Attack for Healthcare Systems. *IEEE Transactions on Emerging Topics in Computing*, *12*, 269–280.
Karale, A. (2021). The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. *Internet Things*, *15*, 100420.
Setiawati, Yenny, & Hermanto, Yanto Paulus. (2023). *Stres dalam Perspektif Neurosains: Sebuah Implikasi Teologis dalam Membangun Kesehatan Mental*. *5*, 1. https://doi.org/https://doi.org/10.52220/magnum.v5i1.205