PHASE 2

Student name: S. Jai Sabari Ganesh

College name: Jeppiaar Institute of Technology

College code: 2106

Semester: 05

Course name: Cloud Application Development

Disaster Recovery with IBM Cloud Virtual Server

Innovation

Project: AI-Powered Predictive Analytic

Description:

Implement AI and machine learning algorithms to predict potential disasters and automate proactive recovery measures. This can include analysing historical data, weather patterns, and system performance metrics.

Introduction:

Artificial intelligence (AI) is one such digital technology that is progressively transforming the humanitarian field. Although there is no internationally agreed definition, AI is broadly understood as "a collection of technologies that combine data, algorithms and computing power".

Preparedness:

AI technologies can support humanitarian preparedness as AI systems can be used to analyse vast amounts of data, thus providing essential insights about potential risks to affected populations. These insights can inform humanitarians about such risks before a crisis or humanitarian disaster unfolds. In this regard, predictive analytics, which builds on data-driven machine learning and statistical models, can be used to calculate and forecast impending natural disasters, displacement and refugee movements, famines, and global health emergencies. To date, such systems have performed best for early warnings and short-term predictions. Yet, their potential is significant, as AI systems performing predictive analytics can be instrumental for preparedness.

For example, the Forecast-based Financing programme deployed by the International Federation of Red Cross and Red Crescent Societies (IFRC) enables the swift allocation of humanitarian resources for early action implementation. This programme uses a variety of data sources, such as meteorological data and market analysis, to determine when and where humanitarian resources should be allocated.

Techno-solutionism, or faith in technologies to solve most societal problems, has proven to yield mixed results in the humanitarian field. For instance, studies have shown that focusing on big data analysis for anticipating Ebola outbreaks in West Africa was not always as effective as investing in adequate public health and social infrastructure. Working closely with affected communities – for example, through participatory design – could help to tailor anticipatory interventions to key community needs, thus better informing and preparing humanitarian action before a conflict or crisis unfolds. This can also apply to AI systems used in humanitarian response, as discussed in the following subsection.

Response:

AI systems can be used in ways that may support humanitarian response during conflicts and crises. For instance, recent advances in deep learning, natural language processing and image processing allow for faster and more precise classification of social media messages during crisis and conflict situations. This can assist humanitarian actors in responding to emergencies. In particular, these advanced AI technologies can help identify areas that would benefit from streamlined delivery of assistance to those in need.

For example, the Emergency Situation Awareness platform monitors content on Twitter in Australia and New Zealand to provide its users with information about the impact and scope of natural disasters such as earthquakes, bushfires and floods as they unfold. Similarly, Artificial Intelligence for Disaster Response, an open platform that uses AI to filter and classify social media content, offers insights into the evolution of disasters. Platforms such as these can triage and classify content, such as relevant images posted on social media showing damages to infrastructure and the extent of harm to affected populations, which can be useful for disaster response and management.

Another example is the Rapid Mapping Service, a project jointly developed by the United Nations (UN) Institute for Training and Research, the UN Operational Satellite Applications Programme, and UN Global Pulse. This project applies AI to satellite imagery in order to rapidly map flooded areas and assess damage caused by conflict or natural disasters such as earthquakes and landslides, thus informing the humanitarian response on the ground.

Depending on their design and deployment, AI systems may support humanitarian responses to conflict and crisis. However, much is context-dependent.

Using AI technologies to map areas affected by disasters seems to yield satisfactory results. For instance, the Humanitarian Open Street Map project relies on AI systems capable of mapping areas affected by disasters. This project uses crowdsourced social media data and satellite and drone imagery to provide reliable information about which areas are affected by disaster situations and need prioritization. However, such a project might not produce relevant results in the context of humanitarian responses in situations of armed conflict. For instance, disinformation campaigns may affect access to trustworthy data during armed conflicts. More generally, problems with access to good-quality data, which can be scarce during armed conflict situations, might affect the design and development of AI systems in that context and thereby compromise the suitability of their mapping tools.

Accordingly, while AI technologies may present opportunities to support effective humanitarian relief responses, they should not be understood as a ready-made, "one-size-fits-all" solution for any context within the realm of humanitarian action.
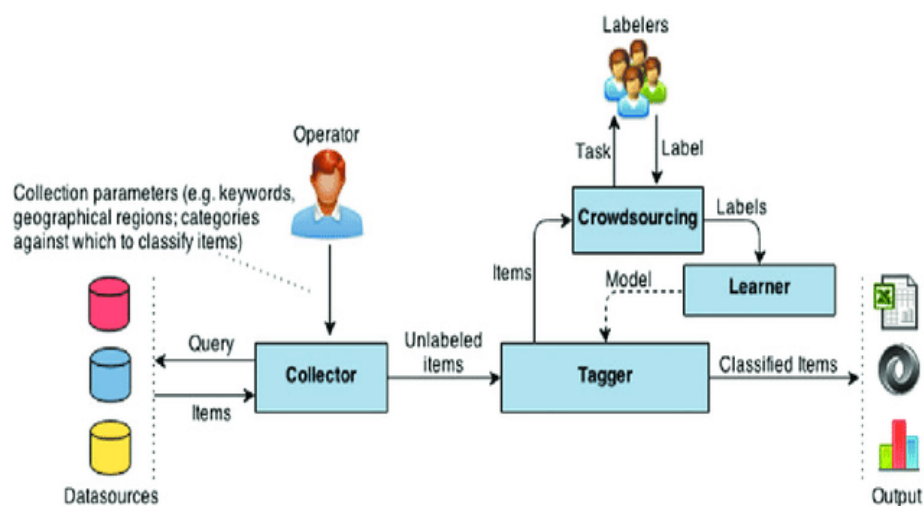
Recovery:

AI may be effectively used in the context of recovery, as the complexities of contemporary crises often lead to protracted conflict situations. Information technology can be an additional asset for facilitating engagement between humanitarians and affected communities in such contexts.

AI technologies may support humanitarian action in protracted situations. For example, the Trace the Face tool developed by the International Committee of the Red Cross (ICRC) was designed to help refugees and migrants find missing family members. This tool uses facial recognition technologies to automate searching and matching, thus streamlining the process. Another example can be found in the AI-powered Chatbot that may provide a way for affected community members to access humanitarian organizations and obtain relevant information. These chatbots are currently providing advisory services to migrants and refugees. Similarly, humanitarian organizations may use messaging chatbots to connect with affected populations.

However, it is vital to question whether it is possible to generalize from these examples that AI contributes to better recovery action. As noted earlier in the analysis of preparedness and response, the benefit of using AI depends very much on the specific context in which these technologies are deployed. This is also true for recovery action.

Community engagement and people-centred approaches may support the identification of areas in which technologies may effectively support recovery efforts on the ground, or conversely, those in which AI systems would not add value to recovery efforts. This should inform decision-making concerning the use of AI systems in recovery programmes. Moreover, AI technologies may also pose considerable risks for affected populations, such as exacerbating disproportionate surveillance or perpetuating inequalities due to algorithmic biases. Such risks are analysed in the following section.

Data Quality:

Concerns about the quality of the data used to train AI algorithms are not limited to the humanitarian field, but this issue can have significant consequences for humanitarian action. In general terms, poor data quality leads to equally poor outcomes. Such is the case, for instance, in the context of predictive policing and risk assessment algorithms. These algorithms often draw from historical crime data, such as police arrest rates per postcode and criminal records, to predict future crime incidence and recidivism risk. If the data used to train these algorithms is incomplete or contains errors, the outcomes of the algorithms (i.e., crime forecasts and recidivism risk scores) might be equally poor in quality. Studies have indeed found that historical crime data sets may be incomplete and may include errors, as racial bias is often present in police records in some jurisdictions such as the United States. If such algorithms are used to support judicial decision-making, it can lead to unfairness and discrimination based on race.

In the humanitarian context, poor data quality generates poor outcomes that may directly affect populations in an already vulnerable situation due to conflicts or crises. AI systems trained with inaccurate, incomplete or biased data will likely perpetuate and cascade these mistakes forward. For instance, a recent study found that ten of the most commonly used computer vision, natural language and audio

data sets contain significant labelling errors (i.e., incorrect identification of images, text or audio). As these data sets are often used to train AI algorithms, the errors will persist in the resulting AI systems.

Unfortunately, obtaining high-quality data for humanitarian operations can be difficult due to the manifold constraints on such operations. For instance, humanitarians may have problems collecting data due to low internet connectivity in remote areas. Incomplete and overlapping datasets that contain information collected by different humanitarian actors may also be a problem – for example, inaccuracies can be carried forward if outdated information is maintained in the data sets. Errors and inaccuracies can also occur when using big data and crowdsourced data. Accordingly, it is crucial that teams working with these data sets control for errors as much as possible. However, data sets and AI systems may also suffer from algorithmic bias, a topic that relates to data quality but has larger societal implications and is thus discussed in the following subsection.

Algorithmic Bias:

Connected to the issue of data quality is the question of the presence of bias in the design and development of AI systems. Bias is considered here not only as a technological or statistical error, but also as the human viewpoints, prejudices and stereotypes that are reflected in AI systems and can lead to unfair outcomes and discrimination. AI systems can indeed reflect the biases of their human designers and developers. Once such systems are deployed, this can in turn lead to unlawful discrimination.

International human rights law prohibits direct and indirect forms of discrimination based on race, colour, sex, gender, sexual orientation, language, religion, political or other opinion, national or social origin, property, birth or other status. Direct discrimination takes place when

an individual is treated less favourably on the basis of one or more of these grounds. Indirect discrimination exists even when measures are in appearance neutral, as such measures can in fact lead to the less favourable treatment of individuals based on one or more of the protected grounds.

Bias in AI systems may exacerbate inequalities and perpetuate direct and indirect forms of discrimination, notably on the grounds of gender and race. For instance, structural and historical bias against minorities may be reflected in AI systems due to the pervasive nature of these biases. Bias also commonly arises from gaps in the representation of diverse populations in data sets used for training AI algorithms. For example, researchers have demonstrated that commercially available facial recognition algorithms were less accurate in recognizing women with darker skin types due in part to a lack of diversity in training data sets. Similarly, researchers have shown that AI algorithms had more difficulties identifying people with disabilities when such individuals were using assistive technologies such as wheelchairs.

In this regard, biased AI systems may go undetected and continue supporting decisions that could lead to discriminatory outcomes. That is partly due to the opacity with which certain machine learning and deep learning algorithms operate – the so-called "black box problem". In addition, the complexity of AI systems based on deep learning techniques entails that their designers and developers are often unable to understand and sufficiently explain how the machines have reached certain decisions. This may in turn make it more challenging to identify biases in the algorithms.

The consequences of deploying biased AI systems can be significant in the humanitarian context. For example, in a scenario where facial recognition technologies are the sole means for identification and identity verification, inaccuracies in such systems may lead to the misidentification of individuals with darker skin types. If identification and identity verification by those means is a precondition for accessing humanitarian aid, misidentification may lead to individuals being denied assistance. This could happen if the system used for triage mistakenly indicates that an individual has

already received the aid in question (such as emergency food supplies or medical care). Such a situation would have dramatic consequences for the affected individuals. If the AI systems' risks were known and not addressed, it could lead to unlawful discrimination based on race. This could also be contrary to the humanitarian principle of humanity, according to which human suffering must be addressed wherever it is found.

Accordingly, safeguards must be put in place to ensure that AI systems used to support the work of humanitarians are not transformed into tools of exclusion of individuals or populations in need of assistance. For example, if online photographs of children in war tend to show children of colour with weapons (i.e., as child soldiers) disproportionately more often, while depicting children of white ethnic background as victims, then AI algorithms trained on such data sets may continue to perpetuate this distinction. This could in turn contribute to existing biases against children of colour in humanitarian action, compounding the suffering already inflicted by armed conflict. Awareness and control for this type of bias should therefore permeate the design and development of AI systems to be deployed in the humanitarian context. Another example relates to facial recognition technologies – as long as these technologies remain inaccurate in recognizing people with darker skin types, they should not be used to assist decision-making essential to determining humanitarian aid delivery.

Data Privacy:

As is internationally agreed, "the same rights that people have offline must also be protected online". This should include AI systems.

International human rights law instruments recognize the right to privacy. In addition, specific legal regimes, such as the General Data Protection Regulation (GDPR), establish fundamental standards for protecting personal data. While the GDPR is a European Union (EU)

law regime that does not bind all humanitarian actors across the globe, it remains relevant beyond the EU as it has inspired similar regulations worldwide.

The principles set forth in the GDPR have also been taken into account by the Handbook on Data Protection in Humanitarian Action, which is considered a leading resource that sets a minimum standard for processing personal data in the humanitarian context. These principles include lawfulness, fairness and transparency in the processing of personal data (Article 5 of the GDPR).

Having a lawful basis for the processing of personal data is a legal requirement (Article 6 of the GDPR). Consent is often used as a lawful basis for processing personal data in the humanitarian context. According to the legal standards, consent must be fully informed, specific, unambiguous and freely given (Article 4(11) of the GDPR). Yet, in the humanitarian context, consent may not be entirely unambiguous and freely given due to the inherent power imbalance between humanitarian organizations and beneficiaries of humanitarian assistance. A refusal to consent to collecting and processing personal data may, in practical terms, lead to the denial of humanitarian assistance. However, it may be difficult for humanitarian actors to ensure that recipients of humanitarian assistance effectively understand the meaning of consent due to linguistic barriers and administrative and institutional complexities.

Fully informed, specific, unambiguous and freely given consent may also be challenging to achieve given that AI systems often use data to further refine and develop other AI solutions. While individuals may agree to have their personal information processed for a specific purpose related to humanitarian action, they may not know about or agree to that data being later used to develop other AI systems. Such

concerns are further aggravated by the criticisms concerning "surveillance humanitarianism", whereby the growing collection of data and uses of technologies by humanitarians may inadvertently increase the vulnerability of those in need of assistance.

These practices require even more scrutiny due to the increasingly common collaborations between technology companies and humanitarian organizations. These companies play a central role in this area as they design and develop the AI systems that humanitarians later deploy in the field. Arguably, technology companies' interests and world view tend to be predominantly reflected in the design and development of AI systems, thus neglecting the needs and experiences of their users. This is particularly concerning for the deployment of AI systems in the humanitarian context, where the risks for populations affected by conflicts or crises are significant. Accordingly, it is essential to have a clear set of guidelines for implementing AI in the humanitarian context, notably placing the humanitarian imperative of "do no harm" at its core, as discussed in the following section.
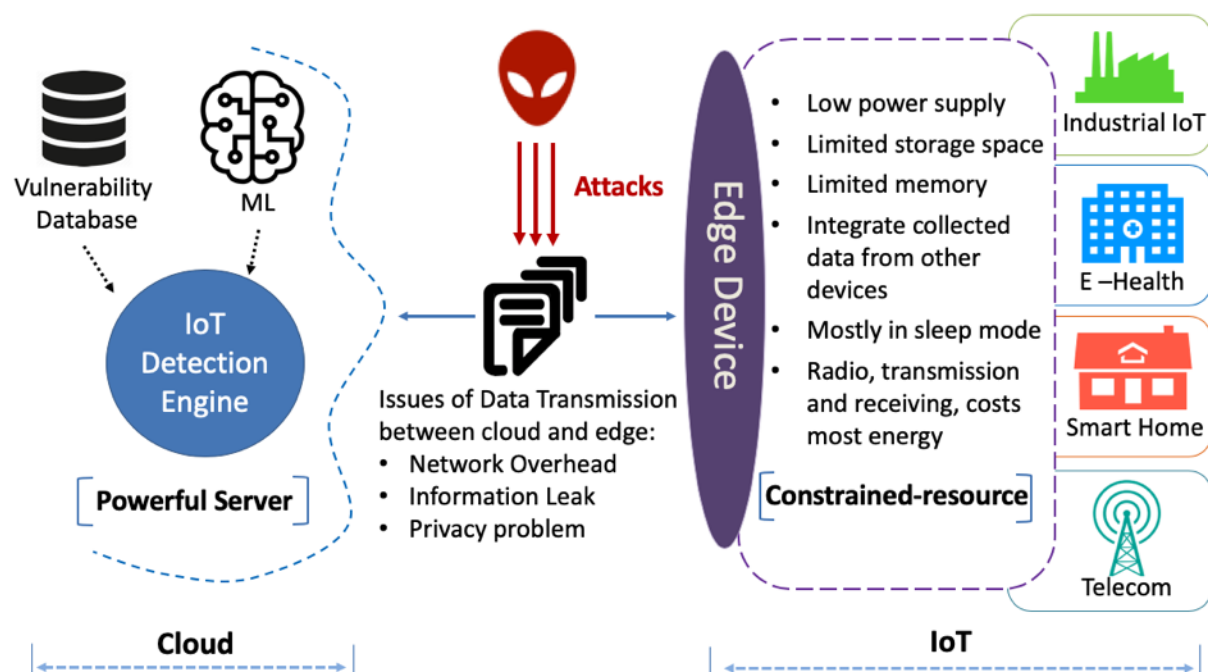
Transparency, Accountability and Redress:

The principle of "do no harm" also implies that humanitarian actors should consider establishing an overarching framework to ensure much-needed transparency and accountability on the uses of AI in humanitarian action.

The term "transparency" is used here to indicate that humanitarian actors should communicate about whether and how they use AI systems in humanitarian action. They should disclose information about the systems they use, even when the way in which these systems work is not fully explainable. In this sense, transparency is a broader concept than the narrower notion of explain ability of AI systems.

For example, consider a scenario in which AI systems are used for biometric identity verification of refugees as a condition for distributing aid in refugee camps. In this case, the humanitarian actors using such AI systems should communicate to the refugees that they are doing so. It is equally important that they disclose to those refugees how they are employing the AI systems and what it entails. For instance, they should disclose what type of information will be collected and for what purpose, how long the data will be stored, and who will access it. Similarly, they should communicate which safeguards will be put in place to avoid cyber security breaches.

Accountability is understood as the action of holding someone to account for their actions or omissions.98 It is a process aimed at assessing whether a person's or an entity's actions or omissions were required or justified and whether that person or entity may be legally responsible or liable for the consequences of their act or omission.99 Accountability is also a mechanism involving an obligation to explain and justify conduct.

In the humanitarian context, accountability should be enshrined in the relationships between humanitarian actors and their beneficiaries – particularly when AI systems are used to support humanitarian action,

due to the risks these technologies may pose to their human rights. For instance, humanitarian actors should inform their beneficiaries of any data security breach that may expose the beneficiaries' personal information and give an account of the measures taken to remedy the situation. The recent swift response by the ICRC to a data security breach has set an example of good practice in this area. The institution undertook direct and comprehensive efforts to explain the actions taken and inform the affected communities worldwide of the consequences of the cyber security incident.

Finally, individuals should be able to challenge decisions that were either automated or made by humans with the support of AI systems if such decisions adversely impacted those individuals' rights. Grievance mechanisms, either judicial or extra-judicial, could thus provide legal avenues for access to remedy, notably in cases where inadvertent harm was caused to the beneficiaries of humanitarian assistance. Extra-judicial mechanisms such as administrative complaints or alternative dispute resolution could be helpful to individuals who may not be able to afford the costs of judicial proceedings.

Conclusion:

In summary, our innovative approach to disaster recovery within the IBM Cloud environment promises to usher in a new era of resilience and efficiency for organizations. By leveraging the power of IBM Cloud services and emerging technologies, we can reimagine disaster recovery as a proactive, real-time, and automated process.

This innovation not only enhances the speed and reliability of recovery efforts but also provides a cost-effective and scalable solution. With a multi-faceted strategy that includes real-time monitoring, automated failover, blockchain-based data integrity, and

the seamless integration of AI and predictive analytics, we are poised to safeguard business continuity in the face of adversity.

Our vision for IBM Cloud disaster recovery is one that empowers organizations to recover swiftly, maintain data integrity, and confidently navigate unforeseen challenges. By embracing these innovations, we not only secure our digital assets but also fortify our ability to adapt and thrive in an ever-evolving technological landscape.