PHASE2

Studentname:S. Abhishekaraj

Collegename: JeppiaarInstitute ofTechnology

College code:2106

Semester:05

Coursename: Cloud

ApplicationDevelopment**DisasterRecoverywithIBM**

CloudVirtualServerInnovation

Project:AI-PoweredPredictiveAnalytic

Description:

ImplementAIandmachinelearningalgorithmstopredictpotentialdisastersandautomateproactiverecoverymeasures.Thiscanincludeanalysing historical data, weather patterns, and system performancemetrics.

Introduction:

Artificial intelligence (AI) is one such digital technology that isprogressivelytransformingthehumanitarianfield.Althoughther eisno internationally agreed definition, AI is broadly understood as “acollection of technologies that combine data, algorithms andcomputingpower”.

Preparedness:

AI technologies can support humanitarian preparedness as AI systemscan be used to analyse vast amounts of data, thus providing essentialinsights about potential risks to affected populations. These insightscan inform humanitarians about such risks before a crisis orhumanitarian 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 healthemergencies. To date, such systems have performed best for earlywarningsandshort-termpredictions.Yet,theirpotentialissignificant,as AI systems performing predictive analytics can be instrumental forpreparedness.

For example, the Forecast-based Financing programme deployed bythe International Federation of Red Cross and Red Crescent Societies(IFRC) enables the swift allocation of humanitarian resources forearly action implementation. This programme uses a variety of datasources, such as meteorological data and market analysis, todetermine when and where humanitarian resources should beallocated.

International Federation
of Red Cross and Red Crescent Societies

Techno-solutionism, or faith in technologies to solve most societalproblems, has proven to yield mixed results in the humanitarian field.Forinstance,studieshaveshownthatfocusingonbigdataanalysisfor anticipating Ebola outbreaks in West Africa was not always aseffective as investing in adequate public health and socialinfrastructure. Working closely with affected communities – forexample,throughparticipatorydesign–couldhelptotailoranticipatory interventions to key community needs, thus betterinforming and preparing humanitarian action before a conflict orcrisisunfolds.ThiscanalsoapplytoAI systemsusedinhumanitarianresponse,asdiscussed inthefollowingsubsection.

Response:

AI systems can be used in ways that may support humanitarianresponse during conflicts and crises. For instance, recent advances indeep learning, natural language processing and image processingallow for faster and more precise classification of social mediamessages during crisis and conflict situations. This can assisthumanitarianactorsinrespondingtoemergencies.Inparticular,theseadvanced AI technologies can help identify areas that would benefitfromstreamlineddeliveryofassistancetothoseinneed.

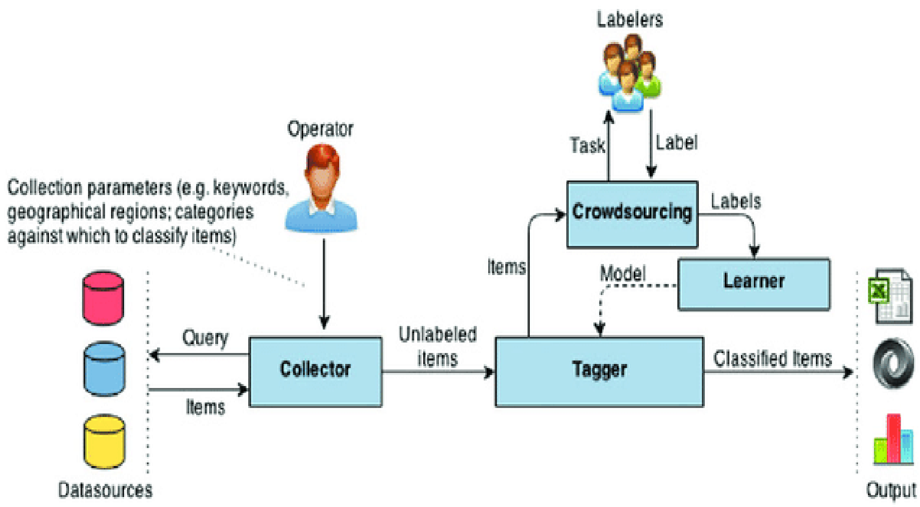
For example, the Emergency Situation Awareness platform monitorscontent on Twitter in Australia and New Zealand to provide its userswithinformationabouttheimpactand scopeofnaturaldisasterssuchas earthquakes, bushfires and floods as they unfold. Similarly,Artificial Intelligence for Disaster Response, an open platform thatuses AI to filter and classify social media content, offers insights intothe evolution of disasters. Platforms such as these can triage andclassify content, such as relevant images posted on social mediashowing damages to infrastructure and the extent of harm to affectedpopulations, which can be useful for disaster response andmanagement.

Another example is the Rapid Mapping Service, a project jointlydeveloped by the United Nations (UN) Institute for Training andResearch, the UN Operational Satellite Applications Programme, andUNGlobalPulse.ThisprojectappliesAItosatelliteimageryinorderto rapidly map flooded areas and assess damage caused by conflict ornatural disasters such as earthquakes and landslides, thus informingthehumanitarian responseon theground.

Dependingontheirdesignanddeployment,AIsystemsmaysupporthumanitarian responses to conflict and crisis. However, much iscontext-dependent.

Using AI technologies to map areas affected by disasters seems toyield satisfactory results. For instance, the Humanitarian Open StreetMap project relies on AI systems capable of mapping areas affectedby disasters. This project uses crowdsourced social media data andsatellite and drone imagery to provide reliable information aboutwhichareasareaffectedbydisastersituationsandneedprioritization.However, such a project might not produce relevant results in thecontext of humanitarian responses in situations of armed conflict. Forinstance, disinformation campaigns may affect access to trustworthydata during armed conflicts. More generally, problems with access togood-quality data, which can be scarce during armed conflictsituations, might affect the design and development of AI systems inthat context and thereby compromise the suitability of their mappingtools.

Accordingly, while AI technologies may present opportunities tosupporteffectivehumanitarian reliefresponses,theyshouldnotbeunderstood as a ready-made, “one-size-fits-all” solution for anycontextwithintherealmofhumanitarian action.



Recovery:

AI may be effectively used in the context of recovery, as thecomplexities of contemporary crises often lead to protracted conflictsituations. Information technology can be an additional asset forfacilitating engagement between humanitarians and affectedcommunitiesin such contexts.

AI technologies may support humanitarian action in protractedsituations. For example, the Trace the Face tool developed by theInternational Committee of the Red Cross (ICRC) was designed tohelp refugees and migrants find missing family members. This tooluses facial recognition technologies to automate searching andmatching, thus streamlining the process. Another example can befound in the AI-powered Chatbot that may provide a way for affectedcommunity members to access humanitarian organizations and obtainrelevant information. These chatbots are currently providing advisoryservices to migrants and refugees. Similarly, humanitarianorganizations may use messaging chatbots to connect with affectedpopulations.

However, it is vital to question whether it is possible to generalizefrom these examples that AI contributes to better recovery action. Asnoted earlier in the analysis of preparedness and response, the benefitofusingAIdependsverymuchonthespecific contextinwhichthesetechnologiesaredeployed.Thisisalsotruefo rrecoveryaction.

Community engagement and people-centred approaches may supportthe identification of areas in which technologies may effectivelysupport recovery efforts on the ground, or conversely, those in whichAI systems would not add value to recovery efforts. This shouldinformdecision-makingconcerningtheuseofAIsystemsinrecoveryprogrammes. Moreover, AI technologies may also pose considerablerisks for affected populations, such as exacerbating disproportionatesurveillanceorperpetuatinginequalitiesduetoalgorithmicbiases. Suchrisksareanalysedinthefollowingsection.

DataQuality:

Concerns about the quality of the data used to train AI algorithms arenot limited to the humanitarian field, but this issue can havesignificant consequences for humanitarian action. In general terms,poor data quality leads to equally poor outcomes. Such is the case, forinstance, in the context of predictive policing and risk assessmentalgorithms. These algorithms often draw from historical crime data,such as police arrest rates per postcode and criminal records, topredict future crime incidence and recidivism risk. If the data used totrain these algorithms is incomplete or contains errors, the outcomesof the algorithms (i.e., crime forecasts and recidivism risk scores)might be equally poor in quality. Studies have indeed found thathistorical crime data sets may be incomplete and may include errors,as racial bias is often present in police records in some jurisdictionssuch as the United States. If such algorithms are used to supportjudicial decision-making, it can lead to unfairness and discriminationbasedon race.

In the humanitarian context, poor data quality generates pooroutcomesthatmaydirectlyaffectpopulationsinanalreadyvulnerablesituation due to conflicts or crises. AI systems trained with inaccurate,incomplete or biased data will likely perpetuate and cascade thesemistakes forward. For instance, a recent

study found that ten of
themostcommonlyusedcomputervision,naturallanguageandaud
io

data sets contain significant labelling errors (i.e., incorrectidentification of images, text or audio). As these data sets are oftenusedtotrainAIalgorithms,theerrorswillpersistintheresulting AIsystems.

Unfortunately, obtaining high-quality data for humanitarianoperations can be difficult due to the manifold constraints on suchoperations.Forinstance,humanitarians mayhaveproblemscollectingdata due to low internet connectivity in remote areas. Incomplete andoverlapping datasets that contain information collected by differenthumanitarian actors may also be a problem – for example,inaccuracies can be carried forward if outdated information ismaintained in the data sets. Errors and inaccuracies can also occurwhen using big data and crowdsourced data. Accordingly, it is crucialthat teams working with these data sets control for errors as much aspossible. However, data sets and AI systems may also suffer fromalgorithmic bias, a topic that relates to data quality but has largersocietalimplicationsandisthusdiscussedinthe followingsubsection.

AlgorithmicBias:

Connectedtotheissueofdataqualityisthequestionofthepresence of bias in the design and development of AI systems. Bias isconsidered here not only as a technological or statistical error, butalso as the human viewpoints, prejudices and stereotypes that arereflected in AI systems and can lead to unfair outcomes anddiscrimination. AI systems can indeed reflect the biases of theirhuman designers and developers. Once such systems are deployed,thiscanin turnlead tounlawful discrimination.

International human rights law prohibits direct and indirect forms ofdiscrimination based on race, colour, sex, gender, sexual orientation,language,religion,politicalorotheropinion,nationalorsoci alorigin,property,birthorotherstatus.Directdiscriminationtakesplace when anindividualistreatedlessfavourablyonthebasisofoneormoreoft hesegrounds.Indirectdiscriminationexistsevenwhenmeasuresar ein appearance neutral, as such measures can in fact lead to the less favourabletreatmentof individualsbasedonone or moreoftheprotectedgrounds.

Bias in AI systems may exacerbate inequalities and perpetuate direct andindirect forms of discrimination, notably on the grounds of gender and race. Forinstance, structural and historical bias against minorities may be reflected inAI systems due to the pervasive nature of these biases. Bias alsocommonly arises from gaps in the representation of diversepopulations in data sets used for training AI algorithms. For example,researchers have demonstrated that commercially available facialrecognition algorithms were less accurate in recognizing women withdarkerskintypesdueinparttoalackofdiversityintrainingdatas ets.Similarly, researchers have shown that AI algorithms had moredifficulties identifying people with disabilities when such individualswereusingassistivetechnologiessuchas wheelchairs.

In this regard, biased AI systems may go undetected and continuesupporting decisions that could lead to discriminatory outcomes. Thatis partly due to the opacity with which certain machine learning anddeeplearningalgorithmsoperate–theso-called“blackboxproblem”. In addition, the complexity of AI systems based on deeplearning techniques entails that their designers and developers areoften unable to understand and sufficiently explain how the machineshave reached certain decisions. This may in turn make it morechallengingto identifybiases inthealgorithms.

Theconsequencesofdeployingbiased AIsystemscanbesignifican tin the humanitarian context. For example, in a scenario where facialrecognition technologies are the sole means for identification andidentity verification, inaccuracies in such systems may lead to themisidentification of individuals with darker skin types. Ifidentification and identity verification by those means is aprecondition for accessing humanitarian aid, misidentification maylead to individuals being denied assistance. This could happen if

thesystemusedfortriagemistakenlyindicatesthatanindividualha
s

already received the aid in question (such as emergency food suppliesor medical care). Such a situation would have dramatic consequencesfor the affected individuals. If the AI systems' risks were known andnot addressed, it could lead to unlawful discrimination based on race.Thiscouldalsobecontrarytothehumanitarianprincipleofhumanity,according to which human suffering must be addressed wherever it isfound.

Accordingly, safeguards must be put in place to ensure that AIsystems used to support the work of humanitarians are nottransformed into tools of exclusion of individuals or populations inneed of assistance. For example, if online photographs of children inwar tend to show children of colour with weapons (i.e., as childsoldiers) disproportionately more often, while depicting children ofwhite ethnic background as victims, then AI algorithms trained onsuch data sets may continue to perpetuate this distinction. This couldin turn contribute to existing biases against children of colour inhumanitarian action, compounding the suffering already inflicted byarmed conflict. Awareness and control for this type of bias shouldtherefore permeate the design and development of AI systems to bedeployed in the humanitarian context. Another example relates tofacialrecognitiontechnologies–aslongasthesetechnologies remaininaccurate in recognizing people with darker skin types, they shouldnot be used to assist decision-making essential to determininghumanitarianaid delivery.

DataPrivacy:

Asisinternationallyagreed,"thesamerightsthatpeoplehaveoffline mustalsobeprotectedonline".ThisshouldincludeAIsystems.

International human rights law instruments recognize the right toprivacy. In addition, specific legal regimes, such as the General DataProtection Regulation (GDPR), establish fundamental standards forprotectingpersonaldata.Whilethe

GDPRisaEuropeanUnion(EU)

law regime that does not bind all humanitarian actors across theglobe, it remains relevant beyond the EU as it has inspired similarregulationsworldwide.

The principles set forth in the GDPR have also been taken intoaccount by the Handbook on Data Protection in Humanitarian Action,which is considered a leading resource that sets a minimum standardfor processing personal data in the humanitarian context. Theseprinciples include lawfulness, fairness and transparency in theprocessingofpersonal data(Article5oftheGDPR).

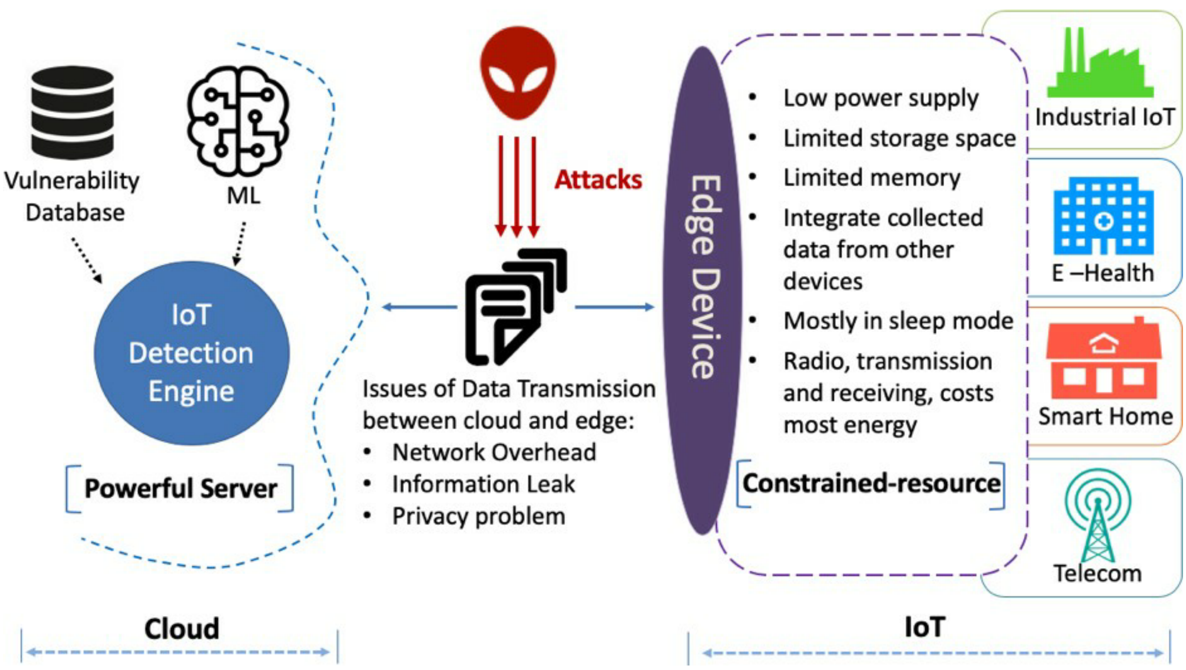
Having a lawful basis for the processing of personal data is a legalrequirement (Article 6 of the GDPR). Consent is often used as alawful basis for processing personal data in the humanitarian context.According to the legal standards, consent must be fully informed,specific, unambiguous and freely given (Article 4(11) of the GDPR).Yet, in the humanitarian context, consent may not be entirelyunambiguous and freely given due to the inherent power imbalancebetweenhumanitarianorganizationsandbeneficiaries ofhumanitarianassistance. A refusal to consent to collecting and processing personaldata may, in practical terms, lead to the denial of humanitarianassistance. However, it may be difficult for humanitarian actors toensure that recipients of humanitarian assistance effectivelyunderstand the meaning of consent due to linguistic barriers andadministrativeand institutionalcomplexities.

Fully informed, specific, unambiguous and freely given consent mayalsobechallengingtoachievegiventhatAIsystemsoftenuseda tatofurther refine and develop other AI solutions. While individuals mayagree to have their personal information processed for a specificpurpose related to humanitarian action, they may not know about

oragreetothatdatabeinglaterusedtodevelopotherAIsystems.Suc
h

concerns are further aggravated by the criticisms concerning“surveillancehumanitarianism”,wherebythegrowingc ollectionofdata and uses of technologies by humanitarians may inadvertentlyincreasethevulnerability ofthoseinneed ofassistance.

These practices require even more scrutiny due to the increasinglycommon collaborations between technology companies andhumanitarian organizations. These companies play a central role inthis areaastheydesignanddeveloptheAIsystemsthathumanitarians later deploy in the field. Arguably, technologycompanies’ interests and world view tend to be predominantlyreflected in the design and development of AI systems, thusneglecting the needs and experiences of their users. This isparticularly concerning for the deployment of AI systems in thehumanitarian context, where the risks for populations affected byconflictsorcrisesaresignificant.Accordingly,itisessentialtohav eaclear set of guidelines for implementing AI in the humanitariancontext, notably placing the humanitarian imperative of “do no harm”atitscore, asdiscussed inthefollowing section.



Transparency,Accountabilityand Redress:

Theprincipleof“donoharm”alsoimpliesthathumanitarianactor sshould consider establishing an overarching framework to ensuremuch-needed transparency and accountability on the uses of AI inhumanitarianaction.

The term “transparency” is used here to indicate that humanitarianactors should communicate about whether and how they use AIsystems in humanitarian action. They should disclose informationabout the systems they use, even when the way in which thesesystemsworkisnotfullyexplainable.Inthissense,transparencyisabroader concept than the narrower notion of explain ability of AIsystems.

For example, consider a scenario in which AI systems are used forbiometric identity verification of refugees as a condition fordistributingaidinrefugeecamps.Inthiscase,thehumanitarianactorsusing such AI systems should communicate to the refugees that theyare doing so. It is equally important that they disclose to thoserefugeeshowtheyare employingtheAIsystemsandwhatitentails.
For instance, they should disclose what type of information will becollected and for what purpose, how long the data will be stored, andwho will access it. Similarly, they should communicate whichsafeguardswillbeputinplacetoavoidcybersecuritybreaches.

Accountability is understood as the action of holding someone toaccount for their actions or omissions.98 It is a process aimed atassessing whether a person's or an entity's actions or omissions wererequired or justified and whether that person or entity may be legallyresponsible or liable for the consequences of their act or omission.99Accountability is also a mechanism involving an obligation to explainandjustify conduct.

In the humanitarian context, accountability should be enshrined in therelationships between humanitarian actors and their

beneficiaries
–particularlywhenAIsystemsareusedtosupporthumanitarianaction,

duetotherisksthesetechnologiesmayposetotheirhumanrights.F or instance, humanitarian actors should inform their beneficiaries ofany data security breach that may expose the beneficiaries' personalinformation and give an account of the measures taken to remedy thesituation. The recent swift response by the ICRC to a data securitybreach has set an example of good practice in this area. The institutionundertook direct and comprehensive efforts to explain the actionstaken and inform the affected communities worldwide of theconsequencesofthecybersecurityincident.

Finally, individuals should be able to challenge decisions that wereeitherautomatedormadebyhumanswiththesupportofAIsy stemsifsuchdecisionsadverselyimpactedthoseindividuals'righ ts.
Grievance mechanisms, either judicial or extra-judicial, could thusprovidelegalavenuesforaccesstoremedy,notablyincaseswh ereinadvertent harm was caused to the beneficiaries of humanitarianassistance. Extra-judicial mechanisms such as administrativecomplaints or alternative dispute resolution could be helpful toindividuals who may not be able to afford the costs of judicialproceedings.

Conclusion:

In summary, our innovative approach to disaster recovery within theIBM Cloud environment promises to usher in a new era of resilienceand efficiency for organizations. By leveraging the power of IBMCloud services and emerging technologies, we can reimagine disasterrecoveryasaproactive,real-time,andautomatedprocess.

This innovation not only enhances the speed and reliability ofrecovery efforts but also provides a cost-effective and scalablesolution. With a multi-faceted strategy that includes real-timemonitoring,automatedfailover,blockchain-baseddataintegrity, and theseamlessintegrationofAIandpredictiveanalytics,wearepoised tosafeguardbusiness continuityinthefaceofadversity.

Our vision for IBM Cloud disaster recovery is one that empowersorganizations to recover swiftly, maintain data integrity, andconfidently navigate unforeseen challenges. By embracing theseinnovations, we not only secure our digital assets but also fortify ourability to adapt and thrive in an ever-evolving technologicallandscape.