Artificial Intelligence (AI) and Machine Learning (ML): IBM Watson for Disaster Response

Sina Najafi
22301645

1. INTRODUCTION

Flood can be considered as a prior example when we talk about a natural disaster. It is characterized by an overflow of water that submerges usually a dry land. It can be result from a heavy rainfall, storms, rapid melting of snow and ice, earthquake, etc. Usually, floods have critical consequences on an urban area, leading to significant loss of life, destruction of property and infrastructures, and long-term economic challenges. As you can see in the following figure, flooding is the most common natural disaster since 1990. From 1990 to 2019, a total of 9,924 natural disasters occurred globally, of which 42 % were floods (IEP, 2020, p.51).

1.1 Figure

Total numbers of global disasters, by disaster type, 1990-2019

Disaster Type	Number of disasters (1990 – 2019)	Percentage (%)
Flood	4119	41.5%
Storm	2942	29.6%
Earthquake	818	8.2%
Landslide	551	5.6%
Extreme temperature	524	5.3%
Drought	475	4.8%
Wildfire	341	3.4%
Volcanic activity	154	1.6%
Total	**9924**	**100%**

Note. From EM-DAT, IEP Calculations. Copyright 2020 by IEB.

Flooding can occur quickly, as in flash floods, which develop within a short time after a heavy rain event, or more gradually, as seen in river floods that result from prolonged heavy rains (Smith, 2010). Specially, urban areas are vulnerable to floods because of high density of population and properties, and prevalence of impermeable surfaces. These surfaces prevent water from naturally infiltrating into the ground, as a result, water will runoff which will, finally, leads to a flood in an urban area.

The consequences of floods are far-reaching. They can cause widespread damage to homes, businesses, and critical infrastructure such as roads, bridges, and power lines. The aftermath of a flood can bring about severe health risks, including waterborne diseases and mental health issues stemming from the loss and trauma experienced by affected populations (WHO, 2018).

But, there can be lots of effective and reliable approaches to mitigate the consequences. Nowadays, flood management and mitigation strategies are crucial to save lives. These solutions can be early warning systems, urban planning, etc. Advancements in technology, particularly in the areas of artificial intelligence and machine learning, have significantly enhanced the ability to predict, detect, and respond to flooding events, thereby reducing their destructive effects in urban areas.

2. RESULTS

Now let’s dive into the technical solution regarding to this disaster and analyze the process of the IBM Watson functioning and then discuss it in the terms of security.

2.1 How IBM Watson Contributes to Urban Resilience and How It Functions

IBM Watson’s AI and ML technologies significantly enhance urban resilience by providing advanced predictive analytics, real-time monitoring as well as efficient response systems, and informed recovery and resilience planning. These three capabilities help cities better prepare for, respond to, and recover from flood events, as a result, reducing the impact of floods on urban populations and infrastructures like hospitals.

2.1.1 Predictive Analytics for Early Warning

Basically, IBM Watson uses data like weather forecasts, satellite imagery, and historical flood data to generate hypotheses and gather massive evidence. Finally, it will initialize a comprehensive analysis, which helps in identifying patterns and predicting potential flood events.

Watson uses advanced machine learning models, such as neural networks and ensemble learning, to predict the likelihood, timing, and severity of floods. These models are continuously trained and refined using new data, improving their predictive capabilities over time (IBM, 2020).

2.1.2 Real-time Monitoring and Response

IBM Watson can complement devices such as, water level sensors to visualize the ongoing conditions of flood, so any unusual pattern can be detected. When this device faces potential flood conditions, it will automatically alert the city. This alert is vital to prepare and have effective response against the disaster.

Watson’s real-time data processing capabilities help in optimizing the deployment of resources, such as emergency services and relief supplies, ensuring they are directed to the areas that need them most (UNDRR, 2019).

2.1.3 Post-Disaster Assessment and Recovery

With image recognition technology we will be able to analyze the captured images from drone and satellite imagery, assessing the damage caused by the disaster. This assessment is needed, when relieving the area is planned. This assessment is also prominent to allocate resource efficiently.

Watson’s analysis provides insights into the most affected areas, enabling better planning for recovery and reconstruction efforts. By understanding the impact of the flood, urban planners can make more informed decisions to rebuild resilient infrastructure (Smith, 2010).

2.2 Context of Use and Infrastructure

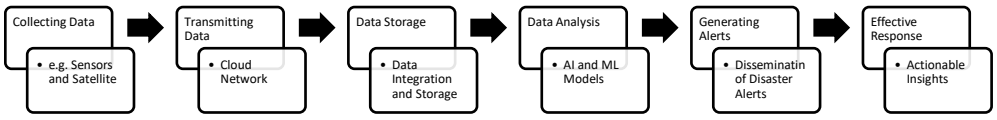
IBM Watson's AI and ML solutions are employed in the context of disaster management, specifically for flood prediction, detection, response, and mitigation. Cities are vulnerable to flooding, particularly benefit from these advanced technologies. These solutions are used by city planners, emergency response teams, government agencies, and environmental organizations to enhance urban resilience against flooding. Of course, necessary infrastructures are needed. Hardware like sensors and IoT devices as well as servers and data centers are required to process and store data. Also, reliable communication networks are necessary when it comes to transfer data from sensors to data centers. This device requires essential software also. Firstly, IBM Watson Platform, the core software that provides AI and ML capabilities. This platform includes tools for data integration, machine learning model development, and deployment (IBM, 2020). Secondly, data integration tools are software for aggregating data from various sources, such as IBM’s Data Refinery (IBM, 2020). Then, there is an analytical tool for data analysis, and finally, alert systems custom software solutions for generating and disseminating alerts to relevant stakeholders (WMO, 2019)

2.2.1 Venice: Predictive Analytics and Real-time Monitoring

Venice has been dealing with frequent and severe flooding, exacerbated by climate change and rising sea levels. The city needed a suitable system to predict and manage these flood events to protect its infrastructure, cultural heritage, and residents. IBM installed a network of sensors across Venice. These devices collect data on tidal movements, weather conditions, and sea levels in real-time. The data from these sensors is transmitted to IBM's cloud-based servers, where it is aggregated and pre-processed using IBM's Data Refinery tools. IBM Watson employs advanced machine learning models to analyze the aggregated data. The models, trained on years of historical flood and weather data, can predict the likelihood and severity of upcoming flood events. These models are continuously updated with new data inputs to enhance their accuracy. The implementation of IBM Watson's AI and ML capabilities in Venice has significantly improved the city's ability to predict and respond to flood events. The advanced warning system and real-time monitoring have enhanced the efficiency of emergency responses, reducing the impact of floods on the city's infrastructure and residents.

2.1 Figure

IBM Watson Flood Management System Architecture



Note. Adopted IBM Watson: How AI and machine learning are improving disaster management, Copyright 2020 by IBM (https://www.ibm.com/watson) , and Flash Flood Guidance System (FFGS), Copyright 2020 WMO(https://community.wmo.int/en/hydrology-and-water-resources/flash-flood-guidance-system-ffgs-global-coverage).

2.3 Main Responsible Entities for IT Crisis Management under BSI

Under the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) in Germany, there are some responsible entities for IT crisis management, especially for advanced solutions in disaster management. These entities play crucial roles in ensuring the security and integrity of IT systems during crises.

2.3.1 Federal Office for Information Security (BSI)

The BSI is the central IT security service provider. It is responsible for protecting government IT systems, developing security standards, and coordinating crisis response (BSI, n.d.). BSI manages risk assessments, develops and enforces security standards, and coordinates response efforts in case of information technology crises. Moreover, BSI has a vital part in protecting digital infrastructure and ensuring the resilience of its information systems against diverse cyber threats. For solutions like IBM Watson in disaster management, BSI is one of the main entities responsible for IT crisis management.

2.3.2 Computer Emergency Response Team for Federal Agencies (CERT-Bund)

CERT Operates under the BSI to respond to security threads affecting federal IT systems. They are responsible in analyzing the risk and applying the process of risk mitigation. Also, another responsibility of this entity is to alerting early warnings.

2.3.3 National Cyber Response Centre (NCAZ)

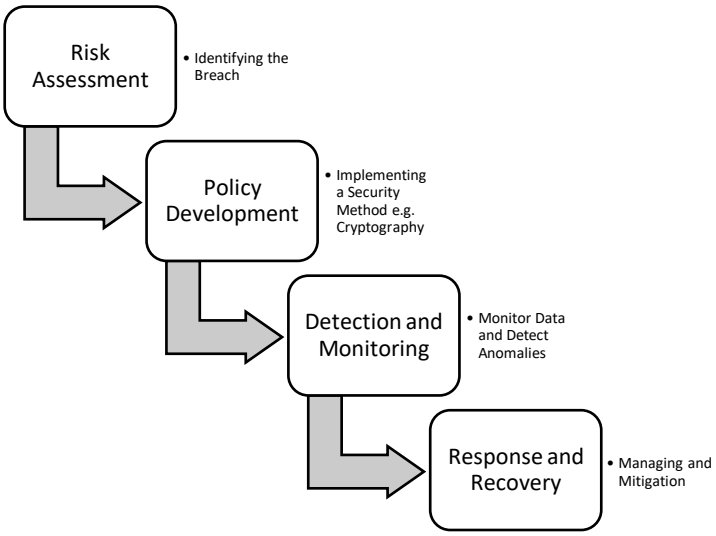
Finally, NCAZ coordinates responses to cyber threats affecting security. NCAZ ensures a coordinated response by bringing together federal agencies, including the BSI, BKA, and intelligence services (BSI, n.d.).

2.4 Security Process for IBM Watson in Disaster Management

For IBM Watson, especially in the context of flood management, security is critical to ensure the integrity and reliability of data and systems. There are several steps to achieve the security when it faces with a threat or risk. These steps include both planning and management roles. A risk could be a ransomware attack, violation of data protection regulations, etc. First step is ***Risk Assessment.*** In the other word, we want to know what the problem or risk is that causing a security breach. Device starts to identify the security risk and vulnerabilities to deploy the required policy. In ***Policy Development,*** security method will be established depending on the type of threat, including cryptography, access control, etc. Then it comes to ***Detection and Monitoring.*** Device uses advanced analytics and ML to monitor data flows and system activities. Then, it Implements an AI algorithms to detect unusual patterns or anomalies that might show a security threat. ***Response and Recovery*** take place with collaboration of different entities and organizations, like NCAZ and CERT to improve the process of managing and mitigating the security breach. Also, restoration of affected systems and services to normal operation would be a priority in this step. These phases ensure a comprehensive approach to maintaining the security and integrity of IBM Watson's systems in disaster management, enhancing resilience and reliability in critical situations. Following figure indicates a brief view of the IBM Watson's security process.

2.2 Figure

IBM Watson in Disaster Management



<-- Image Should be LEFT Aligned!

Note. Adapted from Federal Office for Information Security (BSI), n.d., *Roles and responsibilities in IT security*. Copyright 2024 by BSI. (https://www.bsi.bund.de/EN/Home/home_node.html)

3. DISCUSSION

This part is about process of addressing associated risks with IBM Watson in different categories and evaluating this technical solution, using SWOT analysis.

3.1 Risks and Their Impact on IBM Watson in Disaster Management

Handling these risks is prominent to have successful approach in disaster management with IBM Watson. Following categories show the importance of a comprehensive risk management strategy.

3.1.1 Compliance Risk

Risk: Non-compliance with Data Protection and Privacy Regulations

Non-compliance can cause to major penalties, delay or halt of operation, etc. When IBM Watson deals with data for flood management, restrictions on data usage may limit its capacity to analyze and respond to flood events efficiently.

3.1.2 Hazard Risk

Risk: Natural Disasters e.g. Earthquake

Natural disasters themselves can damage the infrastructure supporting IBM Watson. If the physical infrastructure (e.g., servers, data centers) is damaged during a flood, the system could fail when it is needed the most. This would lead to an inability to provide real-time data and alerts, exacerbating the disaster's impact on the urban area (Federal Office for Information Security (BSI, n.d.).

3.1.3 Control Risk

Risk: Unauthorized Access to the System

Unauthorized access to the system leads to data breaches or manipulation of data. When the Integrity of data is leaked, it will cause incorrect outcomes and predictions from device. As a result, response to the disaster will be in adequate and lives and infrastructures will be in danger.

3.1.4 Opportunity

Risk: Over-reliance on AI Predictions

In the other word, underestimation of human oversight. Relying solely on IBM Watson's AI predictions without adequate human verification can lead to missed nuances or contextual information that AI might not catch. This could result in suboptimal decision-making and responses to flood events (Hildebrandt, 2020).

3.2 Addressing Risks Using the PACED Framework

Addressing these risks through the PACED framework is necessary for IBM Watson to effectively integrate into flood management systems, ensuring compliance, resilience, security, and balanced decision-making.

For example, to address Non-compliance risk using PACED framework, ***planning*** would be to develop a comprehensive data privacy strategy that aligns with international regulations like GDPR. In this part, the goal is to develop a comprehensive risk management strategy that addresses risk categories.

In evaluating ***alternatives***, we explore different compliance frameworks and select the one that best fits the geographic context. In the other word, we consider various alternatives that can simultaneously mitigate risks across categories. For example, establish geographically distributed data centers would be one alternative.

Next step establishing ***criteria*** to select the best alternatives across all risk categories Criteria for selecting the framework could include legal requirements for compliance risk, cost and ease of implementation for hazard and compliance risk, and stakeholder impact for opportunity.

Then, we ***evaluate*** the selected alternatives through comprehensive testing and review to ensure it meets our needs. For example, for compliance risk we can conduct regular audits and compliance checks.

Finally, ***documentation*** is included to finalize and integrate the chosen strategy regarding the risk, the framework, the evaluation results, and the implementation plan.

3.3 SWOT Analysis

Strengths:

One of the considerable advantages of IBM Watson is that it has the feature of ***flexibility and scalability***. It is capable to be implemented in diverse environments, like cities with different complexity and infrastructures. This will help this device to adopt with urban areas expansion and contribute during or after a flood event.

But probably ***integration*** of IBM Watson with existing infrastructures is its most prominent strength. IBM Watson can be a complement device and integrate with sensors, satellites, etc.

Weaknesses:

The ***deployment*** of IBM Watson for flood disaster management can be ***costly***, involving significant investments in hardware, software, and training. This high initial cost can be a barrier for many municipalities, especially those with limited budgets (Smith, 2020).

There are also ***privacy concerns***, managing all the sensitive data from different sources would be challenge to compile with regulations, like GDPR.

Opportunity:

IBM Watson has the opportunity to ***expand to other types of natural disaster*** and beside flood events, provide a comprehensive disaster management solution for earthquakes, volcanic eruptions, etc. Accordingly, it has an opportunity for more and more ***technological advancements***.

Threat:

As with any technology that relies on extensive data collection and analysis, IBM Watson is vulnerable to ***cyber security*** threats. Cyber-attacks could compromise the system, leading to inaccurate predictions or disruptions in disaster response efforts (Jones, 2020).

On the other hand, ***regulatory changes*** of cyber security and protection, can affect the functioning process of the device. For example, adapting to newly derived regulations needs more resources and more operations.

4. REFERENCES

Institute for Economics & Peace. (2020). *Ecological Threat Register 2020: Understanding Ecological Threats, Resilience and Peace*. Sydney. From http://visionofhumanity.org/reports Accessed (6/26/2024)

Smith, J. (2010). *Understanding floods: Causes, effects and options for control.* Rout ledge.

World Health Organization. (2018). *Floods and health.* From https://www.who.int/news-room/fact-sheets/detail/floods

IBM. (2020). *IBM Watson: How AI and machine learning are improving disaster management*. From https://www.ibm.com/watson

UNDRR. (2019). *Global assessment report on disaster risk reduction*. From https://gar.undrr.org/

WMO. (2019). *World Weather Information Service: Flood forecasting and warning.* From https://community.wmo.int/en/hydrology-and-water-resources/flash-flood-guidance-system-ffgs-global-coverage

World Meteorological Organization. (2020). *Flash Flood Guidance System (FFGS).* From https://community.wmo.int/en/hydrology-and-water-resources/flash-flood-guidance-system-ffgs-global-coverage

Federal Office for Information Security (BSI). (n.d.). *Roles and responsibilities in IT security*. From https://www.bsi.bund.de/EN/Home/home_node.html

Hildebrandt, M. (2020). *Law for Computer Scientists and Other Folk*. Oxford University Press.

Smith, R. (2020). Cost analysis of implementing AI in disaster management. Urban Technology Reports, 15(1), 25-33.

Jones, M. (2020). Cyber security threats to AI systems. Cyber security Review, 23(3), 76-89.