Internet of Things’ Functions and Cloud Computing in Emergency Operations and Natural Disaster Prevention

Nao Endo  
Information Technology Management Y4  
SETU Carlow Campusc00253544@setu.ie

*Abstract*— Cloud computing has played a significant role in disaster prevention and recovery over the course of development in its technology. Internet of Things (IoT) has brought a lot of services that collaborate with cloud technology to detect natural disasters and prevent any serious damage or consequences that are caused by natural disasters. The technology detects the signs of natural disasters, analyse the results, then alert end users about the disasters. Thanks to this technology, it is no doubt to say that people’s lives are protected. Also, cloud computing can save organisations’ lives by providing disaster recovery services. This was an innovative solution to the legacy on-premises disaster recovery services that companies used to have from the past. Cloud-based disaster management has been distributed to companies nowadays and played a significant role in their businesses.

Keywords—cloud computing, IoT, Disaster Recovery as a Service

# Introduction

Natural disasters happen anytime and anywhere in the world where humankinds cannot control them from occurring. They do not only damage lands but also kill people by enormous power of what they generate, therefore it is highly critical to analyse how we can prevent the impact of natural disasters that could happen in the globe. There have been a number of measures that are taken in order to prevent natural disasters by using available and suitable technology; for example, Japan, which has faced catastrophic earthquake impacts in the past decades, has Earthquake Early Warning System where the projected primary motion arrival time and presented earthquake intensities are announced in advance which is based on timely analysis of the earthquake's focus and magnitude using wave form data recorded by seismographs close to the epicentre [1]. Thanks to this technology, people are able to evacuate from the dangerous areas that the system detects that earthquakes would hit in and save their lives. Likewise, alert systems against other disasters such as flood and tsunami are also considered to be distributed to public through government bodies all around the world, also by the use of technology. In particular, recently cloud technology has become common in any business cases, and it is also discussed to be included in many of the existing natural disaster alert systems. Internet of Things (IoT) is one of the popular technologies that utilises cloud technology. The IoT is a network of connected devices that can collect, share, and analyse data without the need for human intervention that offers real-time data and has the potential to completely transform the traditional disaster management system which is expected to increase response coordination and overall process efficiency [2]. In addition, over the decade, organisations all around the world have moved from on-premises servers to cloud services in terms of storing and managing their data. This is because of the rapid rise in popularity of cloud services nowadays and companies understand the benefits of the technology. One of the benefits of switching from on-premises servers to cloud is there is a certain data backup in case of disasters that happen on-site. This report discusses the use cases of IoT for alert systems and cloud computing in disaster management in detail and consists of the analysis of the importance of the technology that contributes to the public that have risks of getting damaged from natural disasters.

# The history and influence of Internet of things (IoT)

## History

Firstly, it is believed that IoT has become widely used in a wide range of services that the general public has gotten used to in their daily lives at this stage. In terms of the development of IoT by looking at the history of it, the term "the Internet of Things" was first used by consumer sensor expert and innovator Kevin Ashton to define the network that links physical things to the Internet [3]. The technology allowed computers to have “senses” which had not existed before the development of IoT, thus businesses or service providers could gather data from any IoT devices that are meaningful to them and make use of the data and transform it into their important piece of the businesses or services, which eventually should benefit the customers and consumers. As more and more connected devices entered the market over the course of the decade that followed, public interest in IoT technology started to surge; for instance, the first smart refrigerator was introduced by LG in 2000, the first iPhone was released in 2007 and Google began developing autonomous vehicles in 2009, and the company released its Nest smart thermostat, which enabled remote management of the central heating system in 2011 [4]. Today, it would not be wrong to state that everyone in the developed countries have ever used or contributed to at least one IoT devices or services in their lives, especially smart home and wearable devices has spread to the general public widely that gives users more convenience and excitements in their daily lives such as Amazon’s Alexa and Apple’s smartwatch. In the foreseeable future, it is estimated that 84% of current IoT deployments either address or have the potential to advance the UN's Sustainable Development Goals, according to a 2018 analysis of more than 640 IoT deployments conducted by the World Economic Forum in partnership with research firm IoT Analytics [4].

## Influence

It is also critical to comprehend the reasons for the rapid development and adoption of IoT in the past few decades. There are several advantages that IoT bring with to the public, and in terms of the utilization in natural disaster management, it could be improved security and safety which indicates that the IoT can assist in monitoring and reacting to emergency situations more rapidly and efficiently, enhancing public safety [5]. As for natural disaster management, it is considered that five skills are required: prevention, mitigation, preparedness, response and recovery [6]. By effectively planning the development of the applications that use IoT devices that sensor the signals of any types of natural disasters, it is suggested that the technology can support all the five skills needed for the best practice of natural disaster management. Because manual and analog work of natural disaster management is typically time-consuming and waste of resources, therefore it would not be sufficient and suitable for satisfying the five steps of the management skills. Additionally, it would not provide great security and safety to the public, therefore it could be a huge threat for the public that manual disaster management systems could potentially fail to save lives. Thus, it is discussed that IoT has a significant influence on improving public security and safety by offering the most efficient and convenient way of transferring disaster data to the cloud and forming any sort of information that gives users alert about coming natural disasters.

## IoT and Cloud Computing

Although the term IoT and cloud computing are not exactly identical by definition, it is argued that cloud computing plays a significant assisting role in IoT application. Businesses can access their data from anywhere at any time by storing it on remote servers and the cloud technology facilitates continuous device connectivity and guarantees real-time data sharing. With cloud services, developers may also design unique IoT solutions without requiring extensive hardware or programming experience. Professional services are available for using databases and machine learning technologies from cloud service providers such as AWS and Azure [7].

# Technical Architecture of IoT and Cloud integration

It is argued that the capacity to create, implement, operate, and administer IoT device programs online via the Cloud is essentially what sets the Cloud-based Internet of Things apart from the traditional Internet of Things. Figure 1 represents the integration of both technologies with several supporting technological frameworks.

## Network Protocol in IoT and cloud integration In the architecture of IoT and cloud technology, CoAP is used to interact with each other. A specific web transfer protocol called limited Application Protocol (CoAP) is designed for usage with limited nodes and networks in the Internet of Things, where the goal is to make it possible for basic, limited devices to connect to the Internet of Things despite limited networks' low availability and capacity. Machine-to-machine (M2M) applications like smart energy and building automation are its common applications. The Internet Engineering Task Force (IETF) created the protocol, and IETF RFC 7252 contains the specifications for CoAP. A specific web transfer protocol called limited Application Protocol (CoAP) is designed for usage with limited nodes and networks in the Internet of Things, where the goal is to make it possible for basic, limited devices to connect to the Internet of Things despite limited networks' low availability and capacity. Machine-to-machine (M2M) applications like smart energy and building automation are its common applications. The Internet Engineering Task Force (IETF) created the protocol, and IETF RFC 7252 contains the specifications for CoAP [8]. A CoAP request includes the resource's identity, the method to be used on it, a payload, the type of Internet media it uses, and any optional metadata. The fundamental CoAP methods of GET, POST, PUT, and DELETE may be simply mapped to HTTP methods [9].

## Networking using

Additionally, 6LowPan is commonly used in the architecture that supports the facilitation of the integration between the two technologies. Every node in a low power wireless mesh network that uses 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) has a unique IPv6 address. As a result, the node can establish a direct, open-standard connection with the Internet. The notion that low-power devices with constrained computing capability should be able to participate in the IoT, and that the Internet Protocol could and should be applied even to the tiniest devices, gave rise to 6LoWPAN [10].

## RESTful API for IoT and Cloud integration

RESTful web services are arguably used in the architecture where IoT devices serve as services and behave as RESTful resources. It is considered that RESTful protocol provides a better performance in the integration compared to the other existing protocol SOAs. Although SOAs are frequently used to describe and realize complicated business flows, they are not well suited for allowing end users to construct ad hoc applications. Instead, SOAs encounter complex functional blocks and service implementations. HTTP is a RESTful protocol that handles resources using defined methods comparable to HTTP such as GET, PUT, POST, and DELETE [11].

## A diagram of a cloud network Description automatically generated

Figure 1: IoT and Cloud integration architecture

# Pros and Cons of Combination of IoT and cloud computing

## Pros

### Scalability

More over 15 billion IoT devices are in operation globally as of 2023, and experts predict the figure will rise to 30 billion by 2030 [13]. Large-scale data processing, storage, and protection systems are necessary to manage them all. Many companies are using the cloud as a solution rather than deploying more gear to increase physical storage. A certain degree of flexibility is possible when moving to the cloud for scalability. Companies can assign critical tasks to the platform hosts and adjust their storage capacity in response to demand. In terms of cloud migration, they have more possibilities to modify their current operation, such as private, public, hybrid, or multi-cloud configurations.

### Cost saving

Businesses can cut costs by combining cloud computing with IoT. Employing cloud-based solutions allows businesses to guarantee access to scalable data storage and analytics capabilities while cutting infrastructure expenses dramatically. IoT sensors gather a lot of data from several sources. For analysis, this data is handled on central cloud systems. Organizations are able to monitor a number of parameters, such as the performance of temperature control systems and energy consumption levels. They can save money because they don't have to install local hardware [7].

## Cons

### Reliability

The consistency and availability of cloud services are referred to as reliability, and they can be impacted by network interruptions, malfunctions, or outages [14]. This concept means particularly important to alert systems in emergency situations as any late response to natural disasters might risk people’s lives in the end of the day. If businesses choose highly reliable cloud providers for their IoT operations, it will give them more reliability of their services. However, failing to select a right cloud provider might result in failing the service itself due to the vendor’s poor network connection management.

### Interoperability

Interoperability is considered to be a major obstacle to the integration of cloud computing with IoT. The two technologies' disparate data formats, security standards, and communication protocols will cause the problem. To solve such problems, common standards and protocols for data sharing between cloud computing resources and IoT devices are said to be crucial [7]. When any new projects that deal with IoT and cloud computing, organisations will be expected to make sure there is no technical issues between the IoT.

# IoT use cases for natural disaster alert

## Earthquakes

### QuakeAlert

Although it is not common to hear about earthquakes in the US, there were 21,316 quakes happened in the past 90 days that detected Magnitude 3 or over [16]. Early Warning Labs, a technological company that was founded in California offers earthquake warning services that are provided through the mobile application and also to other enterprises that long to implement the services into their businesses. Their mission is to reduce costs, increase functionality, and enhance the current earthquake early warning systems [15]. To manage the low-cost mass broadcast of these alerts, EWL is building a stable cloud server architecture and conducting research and creating automated response standards and systems that let users, both public and private, take pre-programmed automatic measures to safeguard individuals and assets. The operation of the system is that the QuakeAlert tech platform are connected to seismic sensors placed along fault lines, then alarms will be sent to the end users [16]. One of the notable things about this technology is that hardware are not required to operate QuakeAlert, and by connecting to a cloud-based system, it will be able to transmit alerts to the user's smartphone or speakers that are under the collaborating organisations through an application [17].

Figure 2: Early Warning Labs Website

### ShakeAlert – Collaboration with Google’s Firebase Cloud Messaging

Another similar service of earthquake alert is provided by ShakeAlert, which is an official business partner of QuakeAlert where data from the the United States Geological Survey (USGS) ShakeAlert Earthquake Early Warning system powers the QuakeAlert app [18]. In fact, Google worked together with the California Governor's Office of Emergency Services (Cal OES) and the USGS to deliver ShakeAlert®-powered earthquake alerts straight to Android smartphones in California [18]. Google also sends notifications to Android phones, but they do it without the need for an app because the operating system of the phone already has a feature called "Earthquake Alert", and Android phones can receive notifications as soon as ShakeAlert detects an earthquake because of a direct connection between the ShakeAlert server and Google [19]. Firebase Cloud Messaging, a free cloud service from Google that enables app developers to deliver messages and notifications to users on several platforms, including iOS and Android, is used by the MyShake app. Given that there are so many cell towers that the warning may be dispersed over, most cellular networks are able to handle the strain of sending out a message simultaneously to thousands of phones whose users downloaded the app [20]. Anywhere in the world that you live, you may take part in the Android Earthquake Alerts System using an Android phone as any Android phone can now function as a little seismometer. Tiny accelerometers built into every smartphone are capable of detecting signals that could point to an earthquake and the phone notifies their earthquake detection server of any movement it perceives when there is a possibility of an earthquake and provides a rough location of the shaking. The server then aggregates data from multiple phones to determine whether an earthquake is occurring [19]. The speed of the notification delivery is highly important in case where any earthquakes happen, and this technology that ShakeAlert supports can achieve the delivery speed at as the fastest level as possible. For example, 20,169 alerts were delivered to smartphones running MyShake in response to the September 19, 2020, magnitude-4.5 El Monte earthquake that impacted the Los Angeles area at a depth of 17 kilometers. The entire delivery time to 80% of the phones was 3.5 seconds from the moment the MyShake servers received the ShakeAlert signal. Google also examined its delivery schedules in relation to the earthquake in El Monte and found out more than 2.2 million people received messages via the system, with 80% of them receiving them in less than five seconds. [20].

## Water Level Control

### SmartLog

In the Netherland, there are more than 1500 bridges and more than 100 kilometers of rivers. To stop floods, the Ministry of Infrastructure and Environment, which is in charge of overseeing their development and upkeep, needs cutting-edge IoT devices and instruments. The Dutch Ministry upgraded their network with the assistance of Smartlog and the Dutch telecommunication company KPN so that they could remotely and in real time manage the water level in many canals [21]. Smartlog converted existing sensors which were based on an antiquated radio protocol into intelligent devices. The sensors can be detected from a distance and gather data regarding the water level. To reduce water flows and stop floods, the Smartlog data platform opens sluices and provides notifications. With regard to IoT applications, the Netherlands is the first nation in the world to have a national LoRa network that is provided by KPN. Another technology firm called Actility offers ThingPark that powers this KPN network, allowing a vast array of devices and applications to be connected, managed, and operated. The sophisticated Smartlog IoT platform processes and routes the vast amounts of data that the sensors gather. The platform controls how sensors, base stations, and applications communicate with one another. Additionally, it offers the operator tools for network management and optimization. The country now has access to far more information than previously thanks to this inexpensive installation, which will enhance quality and efficiency of the service.

## Planet Monitoring

Another IoT invention has emerged in the Netherland to warn people all over the world about our planet and prevent any natural disasters that could bring a huge damage to the earth. The company Planet offers real-time satellite monitoring with a constant, entirety, high-resolution aerial image of the planet, observed every day. This technology allows the capability to gather more than 300 million square kilometres of imagery every day. The companies support different businesses all over the world to satisfy their needs by providing them satellite images of what they want to monitor. One of the use cases is in an agriculture industry where farmers and agricultural technology businesses are looking to new technology to guarantee sufficient crops. The agricultural technology company in San Fransisco Granular uses directed searching, automated agronomic guidance, anomaly detection, and Planet Monitoring across more than 22 million acres to promote more productive, profitable farming. [22]. Early unusual activities that are detected through this technology will help prevent agricultural businesses to suffer from potential catastrophises that harm their businesses. Additionally, this technology is also considered to be able to monitor any signs of wildfire which damage not only the natural environment but also human lives. Planet make this innovative service possible by the effective use of modern APIs and cloud architectures.

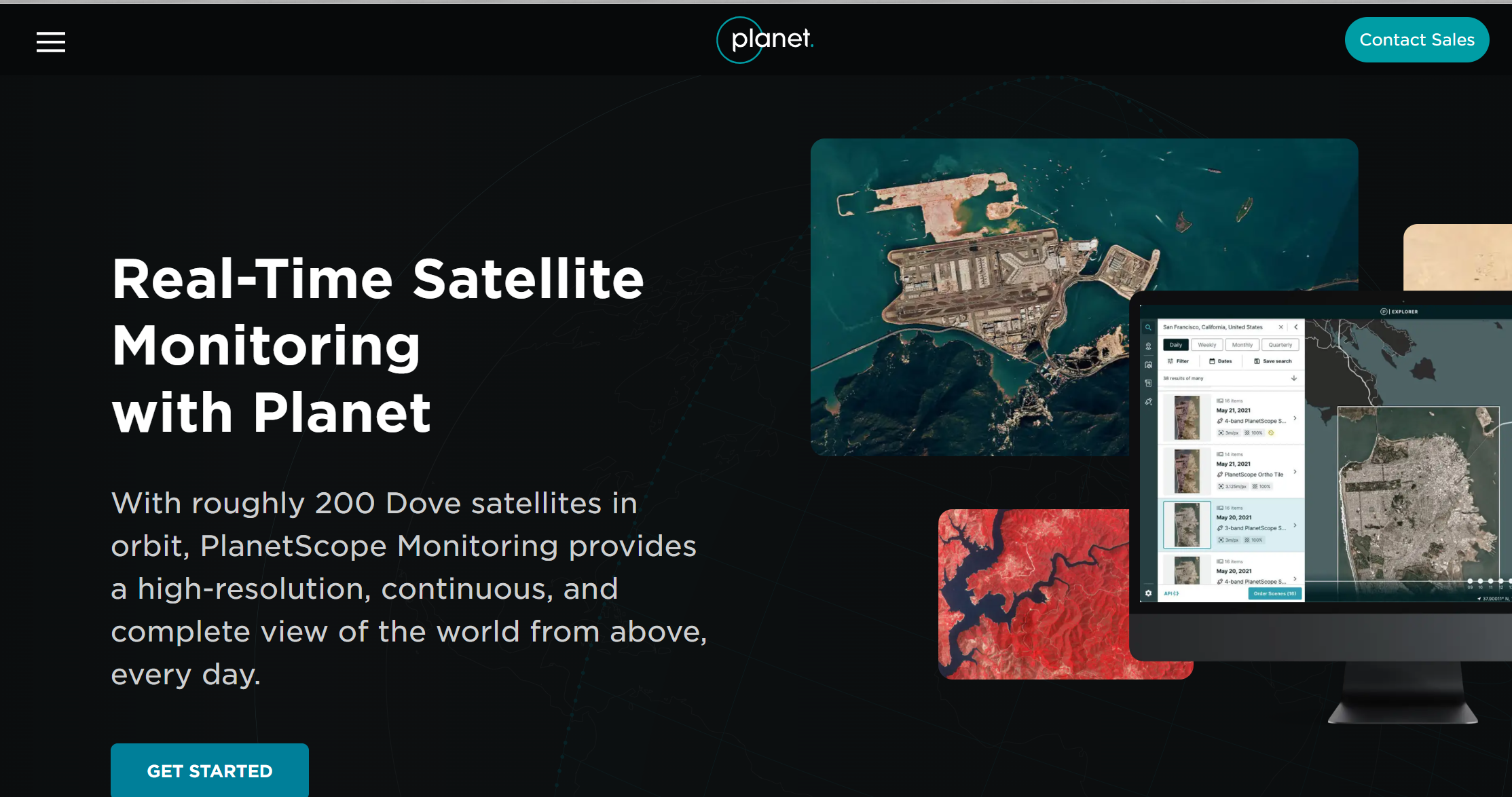


Figure 3: Planet Website

# Evaluation of IoT in disaster mamagement

## The future opportunities of IoT in disaster management

The urgency to develop more robust and effective response systems in the world today is driving an increase in demand for IoT applications in disaster management. In fact, the market for IoT in response to natural disasters has grown significantly in the last several years. The IoT market for natural disaster detection is expected to reach a global market valuation of US$ 18.5 billion by 2034, rising at a compound annual growth rate (CAGR) of 36.3% from 2024 to 2034, according to a Future Market Insights research and in 2023, the market's anticipated market share was approximately US$ 600 million [19]. Also, the number of natural disaster cases happening in the globe has been increasing dramatically in the past decades as the Institute for Economics and Peace's data from 1900 to 2019 shows that there were 396 occurrences in 2019, up from 39 in 1960 [24]. The number is estimated to increase for the foreseeable future as well, therefore the market size is considered to expand accordingly. There are other several factors that businesses could consider joining the market such as there is greater emphasis being placed on proactive methods of disaster relief like early evacuation protocols, and also investments in IoT technology are being prioritized by governments and businesses in order to achieve early warning, quick response, and efficient mitigation of disasters [23].

## Challenges in IoT for Disaster Management

Although it is said that IoT is an innovative technical solution that businesses are recommended to invest in, it is also critical to comprehend the obstacles of the use of IoT in disaster management. For example, implementing and overseeing a sizable number of IoT devices can be a difficult undertaking during widespread disasters because it can be extremely difficult to organize, investigate, and decide based on the massive volume of data produced by IoT devices. Secondly, for more precise seismic ground motion prediction in the context of earthquake and tsunami prediction technology, quick and affordable methods are required. It is necessary to lower the total cost of IoT devices, particularly at the scale required. This is particularly true for developing nations and areas that are frequently hardest hit by natural disasters [23].

# Disaster preparedness with cloud computing

## Disadvantages of On-Premise Solutions

Nowadays, many organisations have worked on preventing attacks from outer environments such like malware, but they have attention to natural disasters too. They are required to prepare for any unexpected situations where their business operation might be affected due to some out-of-blue disasters. When natural disasters damage companies’ on-premises servers, it is certain that there will be consequences that they do not wish to have such as data loss and power outages. Should organisations only have on-premises servers and have some major corruption in their systems, it is considered that it will take a significant amount of time and effort to recover and restore data or system, or it will be possible that they might fail to even come back to the state where they used to be and lead to collapse in their businesses too. Businesses find it difficult to quickly resume full operations following a natural disaster since numerous difficulties frequently arise at the same time. Organizations cannot afford to make internal procedures more difficult in light of the current state of the economy and general infrastructure, thus ignoring cloud technologies puts them at risk for financial losses as well as harm to your brand [25].

## The Backup Strategy

Companies are recommended to implement the 3-2-1 backup strategy in order to protect themselves from facing difficulties in terms of managing their critical data in case of disasters. The rule suggests organisations to make three copies of data, two of which are on-site and one is on a remote location which includes cloud. It is believed that the US government suggests the 3-2-1 backup; Carnegie Mellon proposed the 3-2-1 approach in a US-CERT (United States Computer Emergency Readiness Team) study [26]. By allowing companies to have one backup offsite, it prevents them from losing all data if all the on-site backup data. There are a few other backup strategies that were evolved from the original 3-2-1 method to have an additional security of companies’ data. For example, the 3-2-1+1 backup approach suggests to have 2 copies onsite, one on a remote location, and finally one on cloud in specific. Having as many copies of data as possible is the most recommended, however it is also important to consider the cost and the capacity of data security management. The 3-2-1+1 strategy is considered to be more secure than the original 3-2-1 strategy because should a catastrophe occur, both of the devices where you keep your remote copies will be impacted if they are connected or housed in the same building, therefore it is critical to regularly copy data to the cloud in order to safeguard your files and reduce the quantity of data that is vulnerable.

## Disaster Recovery as a Service

### Overview

Disaster recovery as a service, or DRaaS, is a cloud computing service model that enables an organization to use a SaaS solution to provide all the disaster recovery orchestration and data backup in a third-party cloud computing environment so that IT infrastructure can be accessed and functionally restored following a disaster, where the company may just rely on the service provider and not have to own or manage all the resources needed for disaster recovery [27]. This will let companies have high flexibility and cost saving in terms of disaster preparedness and perform the maximum level of data loss prevention and recovery services. In order for DRaaS to function, servers are replicated and hosted in the facilities of a third-party vendor rather than in the actual location of the company that is responsible for the workload. Should a disaster occur that prevents a customer's site from operating, the disaster recovery plan is carried out on the facilities of the third-party vendor. One of the success stories of the implementation of DRaaS in an organisation happened in the US. Before Hurricane Harvey wreaked havoc in Texas and Louisiana in August of 2017, one of Columbus Global's clients transferred their whole ERP system to the cloud. Their prompt disaster recovery plan allowed them to carry on with business operations even in the event that power and internet failures prevented their on-premises servers from operating [28].

### Recovery as a Service Strucuture

The structure of Database Recovery as a Service (DRaaS) can differ from one vendor to another. This is one of the service providers Vast Edge, which is a business partner of Oracle. Possessing the knowledge and abilities to develop, implement, operate, and maintain the Oracle Cloud Platform for both Oracle and non-Oracle workloads, this organisation was one of the first partners to adopt Oracle cloud in 2016 and was featured by Oracle in Forbes for their successful customer conversions from on-premises and other clouds to Oracle cloud [29]. Figure 4 represents the DRaaS structure of the service. From analysing the diagram, it can be interpreted that the system makes a copy of the production database that sits on premises and save it on the Oracle cloud, where an intermediate activity that deals with Active Data Guard happens during the backup process, which guarantees enterprise data high availability, data security, and disaster recovery [29]. The backed up database on the cloud also deals with another storage in the same cloud called Storage Cloud where some application and database backup unstructured files sit in.

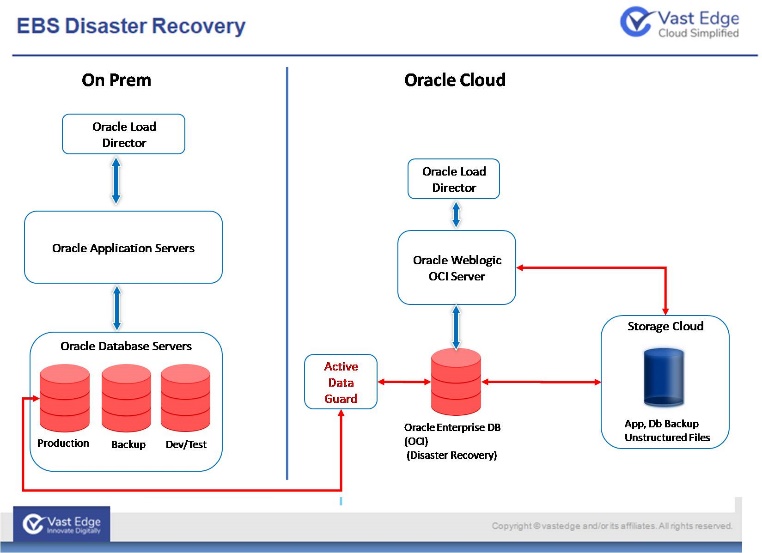


Figure 4: Disaster Recovery Structure

It is suggested that there are a few features that need to be considered by IT managers that deal with disaster recovery. First of all, the most important one is speedy diagnosis. When your service fails to function, it is critical to identify the cause of the issue and find a nearly immediate solution, and to guarantee that your catastrophe recovery happens quickly, your system needs strong and thorough detection. Secondly, it is continual backups because companies may lose dozens or even hundreds of hours of data due to frozen backups, which would need them to start projects again from scratch. Even daily backups might not be enough to meet their demands, depending on the kind of data they handle. For example, data that is classified in the high level of confidentiality need to be backed up more regularly than others. If organisations don't regularly perform backups, their data is always vulnerable to several types of disasters. Finally, securing data storage; whether stored on a disk or on the cloud, firms’ data must be protected from loss, corruption, and malevolent intrusions. Many companies erroneously assume that installing robust firewalls and anti-virus programs is sufficient to safeguard their data, but this is not considered to be the best practice. For data to be secure, oversight, encryption, and routine maintenance are also essential [30]. Therefore, IT managers should implement a rigid policy of who, when, and where the data in cloud is accessible. Especially, if a disaster occurs. it will be a nightmare if the data was unable to recover.

# Limination and challenges of Cloud Computing in Disadter Management

## On-premises vs Cloud

Although disaster management in cloud solutions seems to have a lot of advantages, there are still a few disadvantages that cloud cannot overcome while on-premises can on the other hand. For example, expenses on the DRaaS can be problematic for organisations. DRaaS pricing is based on a subscription model rather than an anticipated upfront cost, and prices may change based on any changes that companies desire, such as additional storage space [31]. Therefore, it is argued that having a rigid plan on choosing the best pricing that suits organisational financial status is crucial for businesses to stay competitive and stable in the market, even though they also would long to have the most secure disaster management. In addition, it is also a drawback that compatibility of applications differs because not every cloud-based recovery service works with every application, particularly ones that are customised for the company [31]. Thus, before companies deploy cloud disaster discovery services, they are expected to have a greater emphasis on the analysis of the services and the applications that the companies use. Otherwise, it will be a failure when disasters actually occur and companies cannot have their data recovered because of the clash between the cloud service and the applications. Also, compared to on-premises, it is considered that latency can be bigger if using cloud services because data recovery is possible in a nearby, yet practical location, which lessens latency-related problems [31].

## Recommendations on cloud based disdter recovery deployment

Following the comprehension of challenges of cloud services in disaster recovery, it is suggested that organisations need to have a high level of planning in order to have a successful deployment. This planning should be aligned with the business plans of each organisation as well. The US government recommends that the business impact analysis, that evaluate and prioritise the disaster factors by the influence, should be used to establish information technology priorities and recovery time goals [32]. However, some argues that this is also a costly process that when you start adding up the monthly costs over a few years, it could not be that much less compared to running a second data centre. This is something that companies might want to avoid financial problems that arise from that. Thereafter, automation and coding will be essential for cloud disaster recovery, unless organisations can afford to just transfer your on-premises data to the cloud [33].

# Conclusion

It is agreeable to state that the impact in the general public that has been brought by the development of cloud computing technologies in disaster prevention or management is significant. For instance, IoT devices that work with cloud can be a life saver for people that might be under danger of natural disasters. IoT devices quickly detects signs of natural disasters, then the data will be analysed and processed in cloud, and finally send alerts or important information to the users. Comprehending the increased number of natural disasters that happen on the globe in recent years, it is considered that the integration of cloud computing in disaster prevention or alerts plays a notable role in the general society for a long term. However, there are still drawbacks in terms of the use of IoT devices in disaster detection that general public or businesses that develop the service need to be cautious of. For example, IoT devices will not communicate with cloud if they lose internet connection or if there was a latency in the communication between them, therefore it is a huge risk should the service fail to deliver alerts when a disaster strikes and kill people’s lives. On the other hand, cloud computing technologies are widely used in Disaster Recovery as a Service where protects organisations from loosing their critical data after disasters occur that damage companies’ data storage systems. It is suggested that the rise in the use of cloud for firms today as opposed to on-premises services is based on a number of reasons that overcome the disadvantages of on-premises solutions. For example, cloud solutions allow companies to have additional environments to secure their data that are supposed to be safe even when disasters occur, therefore the time and effort required for disaster recovery can be much less than having to deal with disaster recovery processes on on-premises servers. It is also crucial to note the drawbacks of Disaster Recovery as a Service as not everything seems to be perfect in this service. It is highly recommended for companies that wish to deploy the service within the businesses to have a intense analysis on how they apply the service into their current systems because there might be a collision between their existing services and the cloud disaster recovery service. Otherwise, the cloud service will not be able to perform the necessary functions that should perform for companies.

##### References

1. Japan Meteorological Agency (2019). *Japan Meteorological Agency*. [online] Jma.go.jp. Available at: <https://www.jma.go.jp/jma/en/Activities/eew1.html>. [Accessed 19 Apr. 2024].
2. ‌FinSMEs (2024). The Role of IoT in Disaster Management andEmergency Response. [online] FinSMEs. Available at: https://www.finsmes.com/2024/03/the-role-of-iot-in-disaster-management-and-emergency-response.html [Accessed 19 Apr. 2024].
3. Gabbai, A. (2015). Kevin Ashton Describes ‘the Internet of Things’. [online] Smithsonian Magazine. Available at: https://www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749/#:~:text=Kevin%20Ashton%20is%20an%20innovator. ‌[Accessed 19 Apr. 2024].
4. Merchant, N. (2021). *IoT Technologies Explained: History, Examples, Risks & Future*. [online] Vision of Humanity. Available at: <https://www.visionofhumanity.org/what-is-the-internet-of-things/>. [Accessed 19 Apr. 2024].
5. www.arduino.cc. (n.d.). *Arduino Education*. [online] Available at: https://www.arduino.cc/education/societal-benefits-of-the-iot. [Accessed 19 Apr. 2024].
6. University of Central Florida (2020). *The Disaster Management Cycle: 5 Key Stages UCF Online*. [online] UCF Online. Available at: https://www.ucf.edu/online/leadership-management/news/the-disaster-management-cycle/. [Accessed 19 Apr. 2024].
7. www.cloudpanel.io. (n.d.). *IoT and Cloud Computing: How Do They Work Together?* [online] Available at: <https://www.cloudpanel.io/blog/iot-and-cloud-computing/>. [Accessed 19 Apr. 2024].
8. Radiocrafts. (n.d.). *CoAP - Constrained Application Protocol*. [online] Available at: <https://radiocrafts.com/technologies/coap-constrained-application-protocol/>. [Accessed 19 Apr. 2024].
9. datatracker.ietf.org. (n.d.). *rfc7252*. [online] Available at: <https://datatracker.ietf.org/doc/html/rfc7252>. [Accessed 19 Apr. 2024].
10. Radiocrafts. (n.d.). *6LoWPAN*. [online] Available at: https://radiocrafts.com/technologies/6lowpan/#:~:text=6LoWPAN%20(IPv6%20over%20Low%2DPower [Accessed 19 Apr. 2024].
11. Zhou, J. (n.d.). *CloudThings: A common architecture for integrating the Internet of Things with Cloud Computing*. Computer Supported Cooperative Work in Design (CSCWD), 2013 IEEE 17th International Conference . [Accessed 19 Apr. 2024].
12. Amos, Z. (2023). How Cloud Computing Improves IoT Scalability. [online] IoT For All. Available at: https://www.iotforall.com/how-cloud-computing-improves-iot-scalability. ‌[Accessed 19 Apr. 2024].
13. Volcanodiscovery. (2024). “*Earthquakes*” [online] Available at: <https://www.volcanodiscovery.com/earthquakes/usa.html> [Accessed 19 Apr. 2024].
14. Early Warning Labs | Earthquake Warning California, Oregon & Washington. (n.d.). *About*. [online] Available at: https://earlywarninglabs.com/old/about-us/ [Accessed 19 Apr. 2024].
15. www.quakelogic.net. (n.d.). *QuakeLogic*. [online] Available at: https://www.quakelogic.net/earthquake-early-warning [Accessed 19 Apr. 2024].
16. ‌www.geoengineer.org. (n.d.). A start up company partners with USGS to launch a new application. [online] Available at: https://www.geoengineer.org/news/a-start-up-company-partners-with-usgs-to-launch-a-new-application [Accessed 19 Apr. 2024]. ‌
17. Early Warning Labs | Earthquake Warning California, Oregon & Washington. (n.d.). *Early Warning Labs - Earthquake Early Warning for California, Oregon, and Washington*. [online] Available at: https://earlywarninglabs.com/ [Accessed 19 Apr. 2024].
18. Google. (2020). *Earthquake detection and early alerts, now on your Android phone*. [online] Available at: https://blog.google/products/android/earthquake-detection-and-alerts/. [Accessed 19 Apr. 2024].
19. Tripathy-Lang, A. (2022). Taking stock of the last decade of earthquake early warning development: what’s next? *Temblor*. doi:https://doi.org/10.32858/temblor.290. [Accessed 19 Apr. 2024].
20. Lavrut, F. (2019). *SmartLog uses LoRa to make Dutch canals smart*. [online] Actility. Available at: https://www.actility.com/smartlog-uses-lora-to-make-dutch-canals-smart/ [Accessed 19 Apr. 2024].
21. Planet Monitoring (2019). *Planet Monitoring*. [online] Planet. Available at: https://www.planet.com/products/monitoring/. [Accessed 19 Apr. 2024].
22. Christian (2024). *IoT in disaster management: Enhancing response and cutting costs*. [online] Ignitec - Product Design Consultancy, Creative Technology and R&D Lab - Ignitec Product Design, Bristol. Available at: https://www.ignitec.com/insights/iot-in-disaster-management-enhancing-response-and-cutting-costs/ [Accessed 19 Apr. 2024].
23. Vision of Humanity (2020). *Global number of natural disasters increases ten times*. [online] Vision of Humanity. Available at: <https://www.visionofhumanity.org/global-number-of-natural-disasters-increases-ten-times/>. [Accessed 19 Apr. 2024].
24. Solutions, M.H., President of Manufacturing, ECI Software (2024). *Disaster Preparedness: A Journey to the Cloud*. [online] Advanced Manufacturing. Available at: <https://www.sme.org/technologies/articles/2024/february/disaster-preparedness-a-journey-to-the-cloud/>. [Accessed 19 Apr. 2024].
25. Campbell, M. (2015). *Why 3-2-1 Backup Sucks*. [online] Unitrends. Available at: https://www.unitrends.com/blog/3-2-1-backup-sucks#:~:text=It%20seems%20like%20every%20backup [Accessed 19 Apr. 2024].
26. VMware (2022). *What is Disaster Recovery as a Service (DRaaS)? | VMware Glossary*. [online] VMware. Available at: <https://www.vmware.com/topics/glossary/content/disaster-recovery-service-draas.html>. [Accessed 19 Apr. 2024].
27. www3.technologyevaluation.com. (n.d.). *Data and Disaster Recovery Planning Using Cloud ERP | TEC*. [online] Available at: <https://www3.technologyevaluation.com/research/article/cloud-erp-and-disaster-recovery-planning.html>. [Accessed 19 Apr. 2024].
28. vastedge.com. (n.d.). *Backup and Disaster Recovery Cloud Services*. [online] Available at: https://vastedge.com/data-center/backup-and-disaster-recovery [Accessed 19 Apr. 2024].
29. Oracle.com. (2022). *Prevent Data Disasters and Corruption*. [online] Available at: <https://www.oracle.com/database/data-guard/>. [Accessed 19 Apr. 2024].
30. lerablog (2015). *5 Necessary Features of a Disaster Recovery Plan*. [online] Lera Blog. Available at: <https://lerablog.org/business/it/5-necessary-features-of-a-disaster-recovery-plan/>. [Accessed 19 Apr. 2024].
31. Lovett, C. (2023). *Disaster Recovery Cloud vs On-Premises | TierPoint*. [online] TierPoint, LLC. Available at: <https://www.tierpoint.com/blog/disaster-recovery-cloud-vs-on-premise/>. [Accessed 19 Apr. 2024].
32. U.S. Department of Homeland Security (2023). *IT Disaster Recovery Plan | Ready.gov*. [online] www.ready.gov. Available at: <https://www.ready.gov/business/emergency-plans/recovery-plan>. [Accessed 19 Apr. 2024].
33. Cloud Computing. (n.d.). *The pros and cons of cloud disaster recovery | TechTarget*. [online] Available at: <https://www.techtarget.com/searchcloudcomputing/feature/The-pros-and-cons-of-cloud-disaster-recovery>. [Accessed 19 Apr. 2024].