EMERGING CLOUD COMPUTING & CLOUD FORENSIC CHALLENGES

CLOUD COMPUTING HISTORY

Cloud computing was invented by Joseph Carl Robnett Licklider in the 1960s, and his purpose was to connect people and data from around the world. Licklider developed APRANet and helped work on Project MAC (Project on Mathematician and Computation)

The goal was to allow users to program a single computer from various locations.

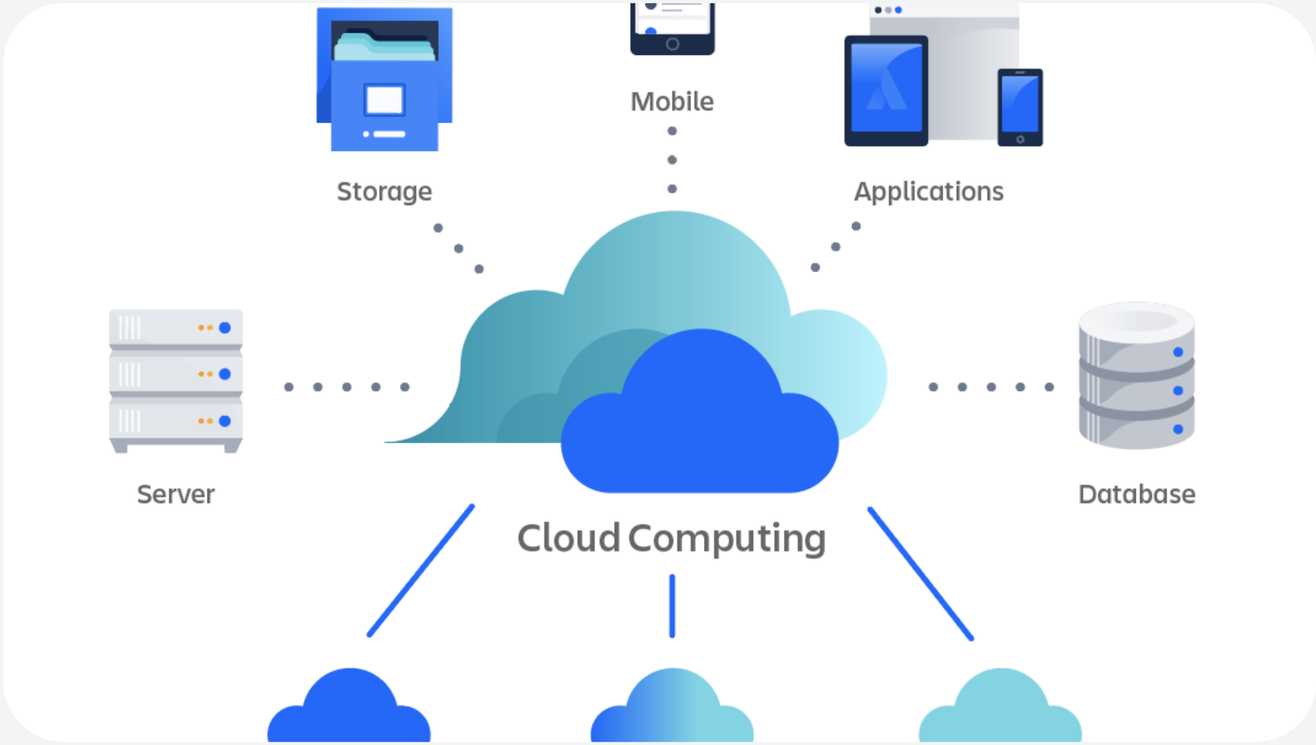
Within 6 months of Project Mac being launched, 200 users were able to access their systems in 10 different MIT locations.
This method of virtual computing started being used in the 90’s and businesses started developing their own cloud service that they offered to consumers.

What Cloud Computing Allows

Cloud Computing allows you to access multiple computer resources, data storage, development tools, and more. It is managed by the cloud service providers which is then delivered over the internet. Cloud computing is divided into three categories which are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

How Cloud Computing Works

Cloud Computing works by allowing clients access to cloud applications over the internet. The companies that provide Cloud services are AWS, Microsoft Azure, Apple, IBM, Google, and Oracle.



Pros of Cloud Computing

There are many advantages of Cloud computing which include the following: It can be cheap since you don’t have to use/pay for more hardware to store your data, cloud Servies can be reliable since your data is stored on multiple servers instead of one. Meaning that if a Hardware failure happens then a consumer's data is not at harm, your data can be backed up and restored on Cloud, cloud can also offer more storage if needed.

Cons of Cloud Computing

The disadvantage of Cloud Computing is that users have limited access, meaning that their data is owned, managed, and monitored by the service provider, cloud is depended on an internet connection. Without a good internet connection, it is hard to access data stored on the Cloud.

AMAZON WEB SERVICES

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Amazon GuardDuty is a continuous security monitoring service. Amazon GuardDuty can help to identify unexpected and potentially unauthorized or malicious activity in your AWS environment.

AWS CloudTrail is an AWS service that helps you enable operational and risk auditing, governance, and compliance of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail.

MICROSOFT AZURE

Microsoft Azure

Azure Virtual Machines are image service instances that provide on-demand and scalable computing resources with usage-based pricing.

Azure Blob Storage is Microsoft's object storage solution for the cloud. Blob Storage is optimized for storing massive amounts of unstructured data.

Azure SQL Database is a fully managed platform as a service (PaaS) database engine that handles most of the database management functions such as upgrading, patching, backups, and monitoring without user involvement

GOOGLE CLOUD PLATFORM

Secure and customizable compute service that lets you create and run virtual machines on Google's infrastructure.

COMPUTE

Cloud Storage is a managed service for storing unstructured data. Store any amount of data and retrieve it as often as you like.

STORAGE

Help protect your applications and websites against denial of service and web attacks.

ARMOR

DIGITAL FORENSICS

Digital forensics is a branch of forensic science that focuses on identifying, acquiring, processing, analysing, and reporting on data stored electronically.

Does not have a defined beginning

Advancements need to be made

WHY MUST A DIGITAL FORENSICS SYSTEM BE STRONG?

System must be able to handle large amounts of data

Must be consistently accessible everywhere

Cybercrime is increasing everyday which means forensics must be stronger

Cloud Forensic Process Flow

Identification: Identification of evidence and incidents that help prove that the events described in the case study actually occurred.

Collection & Preservation: Collect evidence from digital sources such as cell phones, emails, hard drives, and other digital media.

Examination & Analysis: Digital cues are analyzed and evaluated by the device used in the previous phase.

Presentation: The investigator will prepare a report based on the findings.

Cloud Forensics Challenges and Solutions

Maintaining logs: One option is to record in detail every action taken on an instance and use specially designed transport logs to upload those records to a central cloud-based log repository.

Separate plane for cloud data retrieval: Creating a separate plane that would be used to manage the data server required by researchers. Reliable organizations must maintain this cloud infrastructure layer.

Legislative solutions: Create a specific service level agreement (SLA) between customers and cloud service providers (CSP). A SLA should clearly describe the legal requirements to be followed during a criminal investigation.

Cloud Computing Future Trends

Quantum Computing: Quantum computers use the principles of quantum physics to speed up the processing of big data sets and difficult algorithmic tasks.

Edge Computing: Edge computing allows systems to be decentralized and brings processing and data closer to users.

Secure Access Service Edge (SASE): Reduce costs and complexity, provide centralized orchestration and real-time application optimization and help secure seamless access for users.

Green Cloud: A major problem is e-waste, which is produced in large quantities annually by outdated hardware. This is driving the demand for improved computer hardware recycling.

Cloud Computing as it Relates to Digital Forensics
Pros:

- Ability to collect data in real time
- Scalability
  - Computing power
  - Storage
- Accessibility

Cloud Computing as it Relates to Digital Forensics
Cons:

- Direct physical preservation is limited to the suspect’s machine
- Investigators must rely on cloud companies to acquire and preserve data
- Documentation and chain of custody are difficult to achieve in a cloud environment.
- Data is dispersed in the cloud by nature making it difficult to locate and extract.

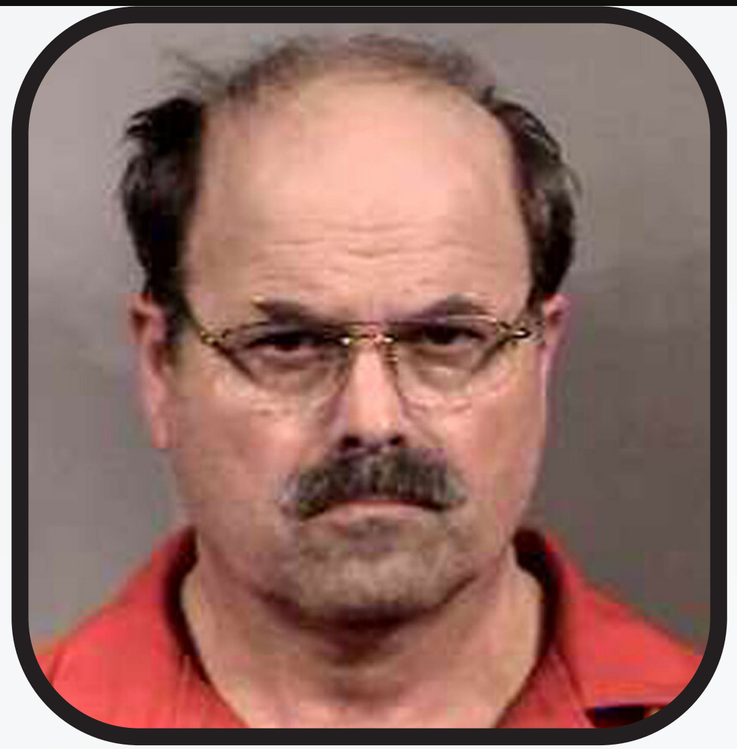
CLOUD COMPUTING ATTACKS

FlexBooker Data Breach

Biggest Data Leak in China

FAMOUS FORENSICS CASE STUDIES

BTK Killer Case



The CraigList Killer

THANK'S FOR WATCHING