Abhisth Chatterji

500084948

R2142201733

B-3 6th Semester

BTech CSE (CCVT) Non-Hons

Week 2: Architectural Styles

Project Title : National DNA Database

Submitted to: Saurabh Shanu Sir

For the creation of National DNA Database, I'll be using AWS. Reasons to select AWS over Azure include:

Customers benefit when a service is offered that they can use for free for a predetermined amount of time in order to get accustomed to and better understand the service. AWS Free-tier can be used to try out the services firsthand without spending a dime. for a full year with particular usage.

Services can be investigated and determined whether their operations are appropriate for using AWS as the platform by exploring the constraints.

On-Demand Pricing Model - Pay-as-you-go pricing from AWS also offers savings on a number of services. Pay just for the individual services as they are needed for the time they are needed, without any cumbersome licensing or long-term commitments.

Most Reliable: Of all cloud computing systems, AWS is intended to be the most trustworthy, flexible, and secure. The core infrastructure safeguards most private data. Data, accounts, and workloads are protected against unauthorized access with the help of services, and the network activity and account behaviour of the cloud environment are constantly watched over.

Fast Pace Innovation: In order to make it easier for clients to adopt the Cloud financially, AWS has created a new lineup of EC2 instances.

Widest Partner Network - AWS has the largest and most active network of partners and clients.

AWS can help with situations including data breaches.

AWS constantly monitors the landscape of privacy laws and regulations for changes and assesses which solutions could be required for our clients to comply with the standards. Customer trust necessitates ongoing dedication. It tries to keep us up to date on the privacy and data security guidelines, practices, and resources we've put in place. Its commitments include:

Access: As a customer, we are solely responsible for configuring access to AWS services, resources, and the content that you upload via your AWS account to the AWS services. We receive a complex set of access, encryption, and logging tools to let us do this successfully.

Storage: The AWS Region(s) in which your content is kept is up to us to choose. In numerous AWS Regions, our content may be backed up and copied.

Security: We have the choice of how to safeguard our content. It gives us the option to keep our encryption keys secret and gives us access to the best encryption techniques available today to protect our content .

Disclosure of customer content: AWS won't divulge customers unless required to by law or court order. AWS will make an effort to refer requests for your custom content from governmental organizations to us.

If AWS is forced by law to expose your custom content to a government agency, it will provide you adequate notice of the requirement so that you can obtain a protective order or another appropriate remedy.

There may be regional variations in information preservation techniques. This can be stopped by creating a central system that various organizations can use and manage so that databases adhere to international standards.

The use of AWS public cloud can be used to accomplish this. The multi-tenant public cloud is constructed. One user can share resources using this design while still protecting their data from other users. For rapid data transmission, the network must be available. It can be used to combine numerous data resources while being reasonably priced. The public cloud allows us to access the cloud remotely from any device.

- It enables companies to spend less on maintenance and capital investments.
- User requests can be easily handled with scalability.
- less resource wastes
- dependable

Public cloud service vendors now offer more advanced security measures. A dedicated crew is engaged to automate security processes and find any anomalies or irregularities in the system. There are strict laws in place to protect user data when it is made available to cloud tenants. In a hybrid system, the public cloud can be used to get permission for higher security levels.

IAM services can assist us in determining the obligations of both professionals and ordinary people.

High Availability and fault tolerance

High availability-like fault tolerance is a standard feature of various AWS services. Some S3 storage levels automatically replicate data across multiple availability zones. If one availability zone is disrupted, data will still be available via the other availability zones without any delays or data loss.Workloads are distributed across a wide range of geographical locations, including several U.S. states, various European countries, and more, thanks to the use of numerous regions.

Depending on the workload, configuring deployment across several availability zones and regions to improve fault tolerance may be difficult. If the workload only consists of data, then data replication over many zones or regions is straightforward.

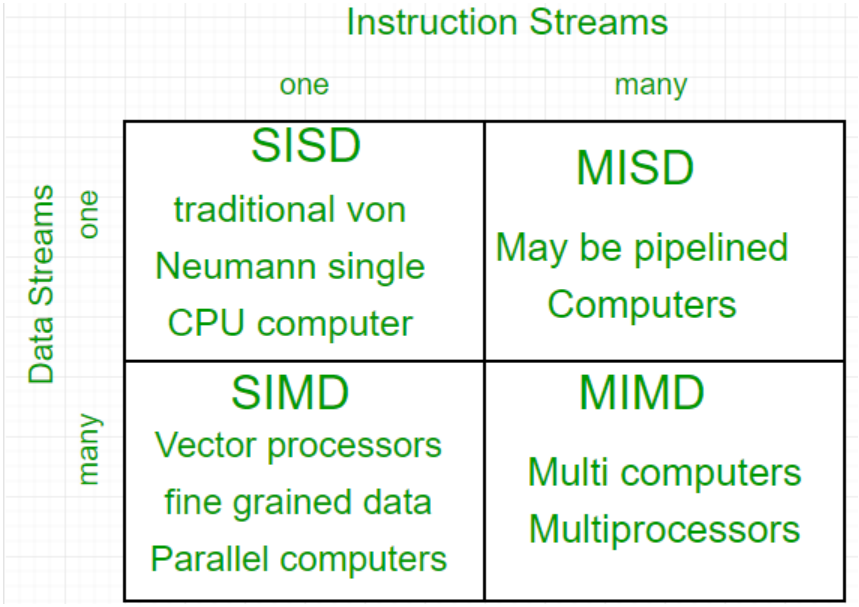
This tactic does not eliminate the possibility of a disruption to the entire location. However, this approach does keep the workload running if one instance fails as a result of a problem with the virtual host infrastructure. Elastic IP addresses, for example, can immediately divert a workload from one EC2 server to another to provide EC2 fault tolerance.

Preserving Acid Properties of Database

A set of characteristics known as "ACID transactions" protects data integrity in database transactions (atomicity, consistency, isolation, and durability). You may securely edit Amazon S3 data at row level by help Athena ACID transactions and support multiple concurrent users. Athena transactions inherently manage coordination and locking semantics; a special record-locking solution is not needed.

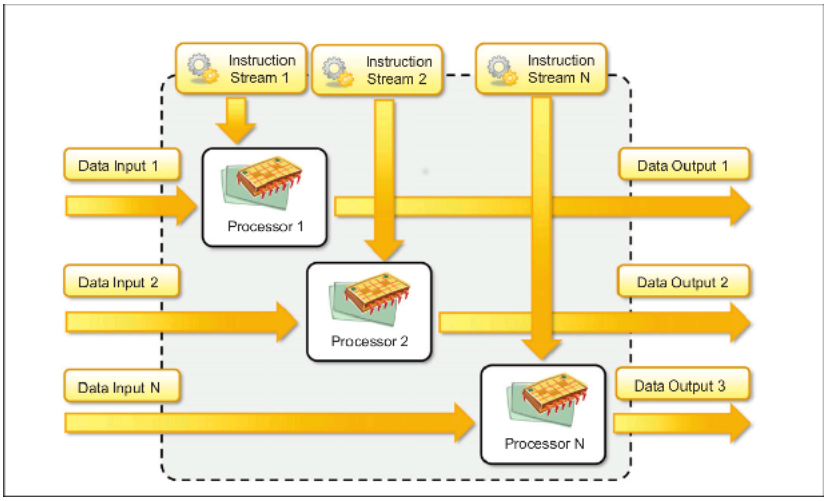
Architectural Styles

There are four major Architectural styles which are known as Flynn's taxonomy.



Source: https://www.geeksforgeeks.org/computer-architecture-flynns-taxonomy/

National DNA database is majorly dependent on a database management system. Since they are able to analyze numerous data sets and handle many activities at once, the majority of database management systems adopt the MIMD classification.



Source : https://www.researchgate.net/figure/MIMD-architecture_fig4_295869570

The MIMD (Multiple Instruction, Multiple Data) architecture is used in database management system to enhance system performance and scalability. The system can handle numerous jobs at once thanks to this architecture, in which each task is carried out by a different processor or core. The MIMD architecture is applied in database management systems in the ways listed below:

Parallel query processing: Complex queries might take a long time to process in a database management system. The query can be broken up into smaller pieces using the MIMD architecture, and each piece can be performed by a different processor or core, leading to quicker execution speeds.

Load balancing: The database management system can distribute the load of incoming requests thanks to MIMD design. the system's overall performance and responsiveness across several processors.

Data Partitioning: The database management system can divide the data into smaller partitions and distribute them across several processors thanks to the MIMD design. Due to the ability to process data in parallel, queries can be executed more quickly.

In a database management system, data replication is used to make sure that the data is accessible even in the event of a failure. The database management system may replicate the data over several nodes thanks to the MIMD architecture, which raises the system's reliability and availability.

In conclusion, database management systems' performance, scalability, and reliability are all significantly enhanced by the MIMD architecture. The system can manage enormous amounts of data efficiently and effectively by enabling parallel processing of complex database operations.

References

1. Rittinghouse, J. W., & Ransome, J. F. (2017, March 27). *Cloud Computing: Implementation, Management, and Security*. CRC Press. https://doi.org/10.1201/9781439806814
2. Furht, B., & Escalante, A. (Eds.). (2010, September 11). *Handbook of Cloud Computing*.
3. Computer Architecture | Flynn's taxonomy - GeeksforGeeks. (2017, December 15). In *GeeksforGeeks*. https://www.geeksforgeeks.org/computer-architecture-flynns-taxonomy/