**DATA PLATFORMS, DATA STORES AND SECURITY**

**ARCHITECTING THE DATA PLATFORM**

A data platform architecture. A layer represents functional components that perform a specific set of tasks in the data platform. The layers that we’re going to explore, include:

Data Ingestion or Data Collection Layer, Data Storage and Integration Layer, Data Processing Layer, and Analysis and User Interface Layer.

**The Data Collection Layer** is responsible for connecting to the source systems and bringing the data from these systems into the data platform. This layer performs the following key tasks: Connect to data sources. Transfer data from these data sources to the data platform in streaming, batch, or both modes. Maintain information about the data collected in the metadata repository. For example, how much data was ingested in a batch, data source, and other descriptive information. Google Cloud DataFlow, IBM Streams, IBM Streaming Analytics on Cloud, Amazon Kinesis, and Apache Kafka are some of the tools used for data ingestion, supporting both batch and streaming modes. Once data is ingested, it needs to be stored and integrated.

**The Storage and Integration layer** in a data platform needs to: Store data for processing and long-term use. Transform and merge extracted data, either logically or physically. Make data available for processing in both streaming and batch modes. The storage layer needs to be reliable, scalable, high-performing, and also cost-efficient. IBM DB2, Microsoft SQL Server, MySQL, Oracle Database, and PostgreSQL are some of the popular relational databases. Cloud-based relational databases, also referred to as Database-as-a-Service, have gained great popularity over the recent years. Such as IBM DB2 on Cloud, Amazon Relational Database Service (RDS), and Google Cloud SQL, and SQL Azure. In the NoSQL, or non-relational database systems on the cloud, we have IBM Cloudant, Redis, MongoDB, Cassandra, and Neo4J. Tools for integration include IBM’s Cloud Pak for Data and Cloud Pak for Integration; Talend’s Data Fabric and Open Studio. Open-source tools such as Dell Boomi and SnapLogic are also very popular integration tools. There are a number of vendors offering cloud-based Integration Platform as a Service (or iPaaS). For example, Adeptia Integration Suite, Google Cloud's Cooperation 534, IBM's Application Integration Suite on Cloud, and Informatica's Integration Cloud. Once the data has been ingested, stored, and integrated, it needs to be processed.

**The processing layer** should be able to: Read data in batch or streaming modes from storage and apply transformations. Support popular querying tools and programming languages. Scale to meet the processing demands of a growing dataset. Provide **a way for analysts and data scientists to work with data in the data platform**. Some of the transformation tasks that occur in this layer include: **Structuring,** essentially, actions that change the form and schema of the data. This change may be as simple as changing the order of fields within a record or dataset or as complex as combining fields into complex structures using joins and unions. **Normalization**, which focuses on cleaning the database of unused data and reducing redundancy and inconsistency. **Denormalization**, which combines data from multiple tables into a single table so that it can be queried more efficiently for reporting and analysis. And **Data Cleaning,** which fixes irregularities in data to provide credible data for downstream applications and uses. There are a host of tools available for performing these transformations on data, selected based on the **data size**, **structure**, and **specific capabilities of the tool**. Such as **spreadsheets, OpenRefine, Google DataPrep, Watson Studio Refinery, and Trifacta Wrangler.** Python and R also offer several libraries and packages that are explicitly created for processing data. **It’s important to note that storage and processing may not always be performed in separate layers.** For example, in relational databases, storage and processing can occur in the same layer, while in Big Data systems, data can be first stored in the Hadoop File Distribution System, or HDFS, and then processed in a data processing engine like Spark. And, **the data processing layer can also precede the data storage layer, where transformations are applied before the data is loaded, or stored, in the database.**

**The Analysis and User Interface Layer** delivers processed data to data consumers. Data consumers can include: Business Intelligence Analysts and business stakeholders who consume this data through interactive visual representations, such as dashboards and analytical reports. Data Scientists and Data Analytics that further process this data for specific use cases. Other applications and services that may need this data as input for further use. The Analysis and UI Layer needs to support: **Querying tools and programming languages**. For example, SQL for querying relational databases and SQL-like querying tools for non-relational databases, such as CQL for Cassandra, Programming languages such as Python, R, and Java, **APIs** that can be used to run reports on data for both online and offline processing. **APIs** that can consume data from the storage in real-time for use in other applications and services. **Dashboarding and Business Intelligence applications**. For example, IBM Cognos Analytics, Tableau, Jupyter Notebooks, Python and R libraries, and Microsoft Power BI.

Overlaying the Data Ingestion, Data Storage and Integration, and Data Processing layers is the **Data Pipeline layer** with the Extract, Transform, and Load tools. This layer is responsible for implementing and maintaining a continuously flowing data pipeline. There are a number of data pipeline solutions available, most popular among them being Apache Airflow and DataFlow.

**Factors for selecting and Designing Data Stores.**

**A data store, or data repository**, is a general term used to refer to data that has been collected, organized, and isolated so that it can be used for business operations or mined for reporting and data analysis.

A repository can be **a database, data warehouse, data mart, big data store, or a data lake**. A well-designed data repository is essential for building a system that is scalable and capable of performing during high workloads.

The primary considerations for designing a data store are:

* The type of data you want to store.
* Volume of data.
* Intended use of data
* Storage considerations.
* Privacy, security, and governance needs of your organization.

**A database** is essentially a collection of data designed for the input, storage, search and retrieval, and modification of data. Depending on the type of data, databases can be categorized in two primary ways – **relational and non-relational.** Relational databases, or RDBMSes, are best used for structured data, which has a well-defined schema and can be organized into a **tabular format**. Non-relational databases, or NoSQL, are best for semi-structured and unstructured data, that is, **schema-less and free-form data**. Non-relational databases, based on the type of data and how you want to query the data, are of **four different types**—**key-value, document, column, and graph-based**. If you're looking to **run complex search queries and multi-operation transactions**, for example, a document-based database may not be the best option for you. Like you would not opt for a graph-based database if you need to process **high-volume transactions** because graph-based databases are not optimized for large-volume analytics queries.

**The volume**, or scale, of data. When you require to store large volumes of raw data in its native format, straight from its source, **a data lake** would be the appropriate choice for you. With a data lake, you can store both relational and non-relational data at scale without defining the data's structure and schema. Or when you're dealing with Big Data, which is data that is not only **high-volume but also high-velocity, of diverse types**, and needs **distributed processing for fast analytics**, then a big data repository would be an option you would explore. Big data stores split large files across multiple computers allowing parallel access to them. Computations run in parallel on each node where data is stored.

**How you intend to use the data you are collecting is also an important consideration for the choice and design of a data store**. The number of transactions, frequency of updates, type of operations performed on the data, response time, and backup and recovery requirements all need to be provisioned for in the design of a data store.

1. **Transactional systems**, that is systems used for capturing high-volume transactions, need to be designed for high-speed read, write, and update operations.
2. **Analytical systems**, on the other hand, need complex queries to be applied to large amounts of historical data aggregated from transactional systems. They need faster response times to complex queries. Schema design, indexing, and partitioning strategies have a big role to play in performance of systems based on how data is getting used.

The intended use of data also drives **scalability** as a design consideration. **The scalability** of a data store is its capability to handle growth in the amount of data, workloads, and users. Normalization of the database is another important consideration at the design stage. **Normalization** is the process of efficiently organizing data in a database. Done right, it helps in the optimal use of storage space, makes database maintenance easier, and provides faster access to data. Normalization is important for systems that **handle transactional data**. But for systems designed for handling analytical queries, normalization can lead to performance issues.

**The perspective of storage**. These are **Performance, Availability, Integrity, and Recoverability of Data**. PAIR

1. **Performance** parameters include throughput and latency. That is, the rate at which information can be read from and written to the storage and the time it takes to access a specific location in storage.
2. **Availability** - Your storage solution must enable you to access your data when you need it, without exception. There should be no downtime.
3. **Integrity** - Your data must be safe from corruption, loss, and outside attack.
4. **Recoverability** - Your storage solution should ensure that you can recover your data in the event of failures and natural disasters.

**A secure data strategy** is a layered approach. It includes **access control, multizone encryption, data management, and monitoring systems**.

**Regulations** such as GDPR, CCPA, and HIPAA restrict the ownership, use, and management of personal and sensitive data. Data needs to be made available through controlled data flow and data management by using multiple data protection techniques. This is an important part of a data store design. Strategies for data privacy, security, and governance regulations need to be a of a data store's design from the start. Done at a later stage it results in patchwork.

**SECURITY**

Three key components to creating an effective strategy for information security in general these are popularly referred to as the **CIA** triad the **C** in this triad stands for **confidentiality** through controlling unauthorized access **I** for integrity through validating that your resources are trustworthy and have not been tampered with and **A** is for availability by ensuring authorized users have access to resources when they need it the

CIA triad is applicable to all facets of security be it infrastructure network application or data security.

The four different facets or levels of security are **Physical Infrastructure**, **Network security, Application security, and Data security.**

**Physical infrastructure** security a key component of security for an it system is the security of the physical infrastructure and facilities that house the system in the case of cloud computing this extends to the **cloud service providers infrastructure and facilities** here are some of the measures that are taken to ensure physical infrastructure security access to the perimeter of the facility based on **authentication and round-the-clock surveillance for entry and exit points** **multiple power feeds** from independent utility providers with dedicated generators and **ups battery backup heating and cooling mechanisms** for managing the temperature and humidity levels in the facility and by factoring in environmental threats before considering the location of the facility for example infrastructure facilities are never housed in **flood plains in areas prone to earthquakes** the infrastructure is housed in an earthquake-resistant structure multi-level lightning protection and earthing systems are also installed in such facilities

**Network security**: network security is vital to keep interconnected systems and data safe network security solutions include **firewalls** to prevent unauthorized access to private networks that are connected to the internet, **network access control** to ensure endpoint security by allowing only authorized devices to connect to the network, for example, a corporate network may not allow devices with outdated service packs to connect to their network segmentation to create silos or virtual local area networks within a network so that you can segregate your assets into individual silos based on the level of security required for different assets **security protocols** to ensure attackers cannot tap into data while it is in transit and **intrusion detection and intrusion prevention** systems that inspect incoming traffic for intrusion attempts and vulnerabilities.

**Application security:** application security is critical for keeping customer data private and ensuring applications are fast and responsive security needs to be built into the foundation of an application in order to prevent other applications and services from introducing vulnerabilities you can make your application safe by following security engineering practices such as **threat modeling** to identify relative weaknesses and attack patterns related to the application, **secure design** that mitigates risks secure coding guides and practices that prevent vulnerabilities and **security testing** to fix problems before the application is deployed and to validate that it is free from known security issues.

**Data security** data is either at rest in storage or in transit between systems applications services and workloads be it at rest or in motion data needs to be protected one of the primary controls for data security is to enable access to data through a **system of authentication and authorization,** authentication systems verify that you are who you say you are and they accomplish this using **passwords tokens biometrics or a combination of these**. Authorization ensures that users access information based on their **roles and the privileges assigned to their roles**. Data at rest includes **files objects and storage** this type of data is stored physically such as in a database, data warehouse, tapes off-site, backups or on mobile devices. Organizations can use **encryption** to fight threats to their data at rest encrypting data protects information from disclosure even if that information is lost or intercepted data that is moving from one place to another such as when it is transmitted over the internet is referred to **as data in transit or data in motion,** encryption methods such as **https ssl and tls** are often used to protect data in motion. The vulnerabilities data can be exposed to and the security features that help protect data end to end through its life cycle it is vital to **proactively monitor track and react to security violations in time** and for that you need end-to-end visibility and integration of security processes and tools throughout the enterprise, **security monitoring and intelligence systems** create a complete audit history for triage and compliance purposes and provide reports and alerts that help enterprises react to security violations in time.

**VIEWPOINTS: IMPORTANCE OF DATA SECURITY**

If your data is not secured, nothing else matters. It can result in dire consequences such as company-ending.

Data security cannot be patched in, It has to be thought of every step of the way.

Give the least privilege needed in order to do their job

**Summary and Highlights**

In this lesson, you have learned:

The architecture of a data platform can be seen as a set of layers, or functional components, each one performing a set of specific tasks. These layers include:

Data Ingestion or Data Collection Layer, responsible for bringing data from source systems into the data platform.

Data Storage and Integration Layer, responsible for storing and merging extracted data.

Data Processing Layer, responsible for validating, transforming, and applying business rules to data.

Analysis and User Interface Layer, responsible for delivering processed data to data consumers.

Data Pipeline Layer, responsible for implementing and maintaining a continuously flowing data pipeline.

A well-designed data repository is essential for building a system that is scalable and capable of performing during high workloads.

The choice or design of a data store is influenced by the type and volume of data that needs to be stored, the intended use of data, and storage considerations. The privacy, security, and governance needs of your organization also influence this choice.

The CIA, or Confidentiality, Integrity, and Availability triad are three key components of an effective strategy for information security. The CIA triad is applicable to all facets of security, be it infrastructure, network, application, or data security.

**Data Collection and Data Wrangling**

Sources of data can be databases, the web, sensor data, data exchanges and several other sources leveraged for specific data needs.

Importing data into different types of data repositories:

**SQL, or Structured Query Language**, is a querying language used for extracting information from relational databases. SQL offers simple commands to specify what is to be retrieved from the database, the table from which it needs to be extracted, grouping records with matching values, dictating the sequence in which the query results are displayed, and limiting the number of results that can be returned by the query, amongst a host of other features and functionalities. **Non-relational databases** can be queried using SQL or SQL-like query tools. Some non-relational databases come with their own querying tools such as CQL for Cassandra and GraphQL for Neo4J.

**Application Programming Interfaces (or APIs)** are also popularly used for extracting data from a variety of data sources. APIs are invoked from applications that require the data and access an end-point containing the data. End-points can include databases, web services, and data marketplaces. APIs are also used for data validation. For example, a data analyst may utilize an API to validate postal addresses and zip codes.

**Web scraping**, also known as screen scraping or web harvesting, is used for downloading specific data from web pages based on defined parameters. Among other things, web scraping is used to extract data such as text, contact information, images, videos, podcasts, and product items from a web property.

**RSS** feeds are another source typically used for capturing updated data from online forums

and news sites where data is refreshed on an ongoing basis.

**Data streams** are a popular source for aggregating constant streams of data flowing from sources such as instruments, IoT devices and applications, and GPS data from cars.

**Data Exchange** platforms allow the exchange of data between data providers and data consumers. Data Exchanges have a set of well-defined exchange standards, protocols, and formats relevant for exchanging data. These platforms not only facilitate the exchange of data, they also ensure that security and governance are maintained. They provide data licensing workflows, de-identification and protection of personal information, legal frameworks, and a quarantined analytics environment. Examples of popular data exchange platforms include AWS Data Exchange, Crunchbase, Lotame, and Snowflake. Numerous other data sources can be tapped into for specific data needs. For marketing trends and ad spending, for example, research firms like Forrester and Business Insider are known to provide reliable data. Research and advisory firms such as Gartner and Forrester are widely trusted sources for strategic and operational guidance. Similarly, there are many trusted names in the areas of user behavior data, mobile and web usage, market surveys, and demographic studies. Data that has been identified and gathered from the various data sources now needs to be loaded or imported into a data repository before it can be wrangled, mined, and analyzed.

Data streams and feeds are also used for extracting data from social media sites and interactive platforms.

**The importing process** involves combining data from different sources to provide a combined

view and a single interface using which you can query and manipulate the data.

Depending on the data type, the volume of data, and the type of destination repository,

you may need varying tools and methods.

**Specific data repositories are optimized for certain types of data**. Relational databases store structured data with a well-defined schema. If you’re using a relational database as the destination system, you will only be able to store structured data, such as data from OLTP systems, spreadsheets, online forms, sensors, network and web logs. **Structured data can also be stored in NoSQL**. Semi-structured data is data that has some organizational properties but not a rigid schema, such as, data from emails, XML, zipped files, binary executables, and TCP/IP protocols. Semi-structured can be stored in NoSQL clusters. XML and JSON are commonly used for storing and exchanging semi-structured data. JSON is also the preferred data type for web services. Unstructured data is data that does not have a structure and cannot be organized into a schema, such as data from web pages, social media feeds, images, videos, documents, media logs, and surveys. NoSQL databases and Data Lakes provide a good option to store and manipulate large volumes of unstructured data. Data lakes can accommodate all data types and schema.

Tools such as Talend and Informatica, and programming languages such as Python and R, and their libraries, are widely used for importing data.

**Data Wrangling**

**Data wrangling, also known as data munging**, is an iterative process that involves data

exploration, transformation, validation, and making data available for a credible and meaningful

analysis.

Key transformation of raw data.

the first transformation task:

1. **Structuring**. This task includes actions that change the form and schema of your data. The incoming data can be in varied formats. You might, for example, have some data coming from a relational database and some data from Web APIs. In order to merge them, you will need to change the form or schema of your data. This change may be as simple as changing the order of fields within a record or dataset or as complex as combining fields into complex structures. **Joins and Unions** are the most common structural transformations used to combine data from one or more tables.

**Joins combine columns**. When two tables are joined together, columns from the first source table are combined with columns from the second source table—in the same row. So, each row in the resultant table contains columns from both tables. **Unions combine rows**. Rows of data from the first source table are combined with rows of data from the second source table into a single table. Each row in the resultant table is from one source table or another.

1. **Normalization and Denormalization of data**. Normalization focuses on cleaning the database of unused data and reducing redundancy and inconsistency. Data coming from transactional systems, for example, where a number of insert, update, and delete operations are performed on an ongoing basis, are highly normalized. Denormalization is used to combine data from multiple tables into a single table so that it can be queried faster. For example, normalized data coming from transactional systems is typically denormalized before running queries for reporting and analysis.
2. **Cleaning. Cleaning** tasks are actions that fix irregularities in data in order to produce a credible and accurate analysis. The first step in the data-cleaning workflow is to detect the different types of issues and errors that your dataset may have. You can use **scripts and tools** that allow you to define specific rules and constraints and validate your data against these rules and constraints. You can also use **data profiling and data visualization tools for inspection**. **Data profiling** helps you to inspect the source data to understand the structure, content, and interrelationships in your data. It uncovers anomalies and data quality issues. For example, blank or null values, duplicate data, or whether the value of a field falls within the expected range. Visualizing the data using statistical methods can help you to spot outliers. For example, plotting the average income in a demographic dataset can help you spot outliers. That brings us to the actual cleaning of the data. The techniques you apply for cleaning your dataset will depend on your use case and the type of issues you encounter.

Let’s look at some of the more common data issues. Let’s start with missing values. **Missing values** are very important to deal with as they can cause unexpected or biased results. You can choose to filter out the records with missing values or find a way to source that information in case it is intrinsic to your use case. For example, missing age data from a demographics study. A third option is a method known as **imputation,** which calculates the missing value based on statistical values. Your decision on the course of action you choose needs to be anchored in what’s best for your use case. You may also come across **duplicate data**, data points that are repeated in your dataset. These need to be removed. Another type of issue you may encounter is that of **irrelevant data**. Data that does not fit within the context of your use case can be considered irrelevant data. For example, if you are analyzing data about the general health of a segment of the population, their contact numbers may not be relevant for you. Cleaning can involve **data type conversion** as well. This is needed to ensure that values in a field are stored as the data type of that field—for example, numbers stored as numerical data type or date stored as a date data type. You may also need to clean your data in order **to standardize it**. For example, for strings, you may want all values to be in lower case. Similarly, date formats and units of measurement need to be standardized. Then there are **syntax errors**. For example, white spaces, or extra spaces at the beginning or end of a string is a syntax error that needs to be rectified. This can also include **fixing typos or format**, for example, the state name being entered as a full form such as New York versus an abbreviated form such as NY in some records. Data can also have **outliers**, or values that are vastly different from other observations in the dataset. Outliers may, or may not, be incorrect. For example, when an age field in a voters database has the value 5, you know it is incorrect data and needs to be corrected. Now let’s consider a group of people where the annual income is in the range of one hundred thousand to two hundred thousand dollars—except for that one person who earns a million dollars a year. While this data point is not incorrect, it is an outlier, and needs to be looked at.

**Tools for Data Wrangling**

Excel Power Query / Spreadsheets and Add-ins OpenRefine Google DataPrep Watson Studio Refinery Trifacta Wrangler Python R.

**Spreadsheets**. Spreadsheets such as Microsoft Excel and Google Sheets have a host of features and in-built formulae that can help you identify issues, clean, and transform data. Add-ins are available that allow you to import data from several different types of sources and clean and transform data as needed—such as Microsoft Power Query for Excel and Google Sheets Query function for Google Sheets.

**OpenRefine** is an open-source tool that allows you to import and export data in a wide variety

of formats, such as TSV, CSV, XLS, XML, and JSON. Using OpenRefine, you can clean data, transform it from one format to another, and extend data with web services and external data.

OpenRefine is easy to learn and easy to use. It offers menu-based operations, which means you don’t need to memorize commands or syntax.

**Google DataPrep** is an intelligent cloud data service that allows you to visually explore, clean, and prepare both structured and unstructured data for analysis. It is a fully managed service, which means you don’t need to install or manage the software or the infrastructure. DataPrep is extremely easy to use. With every action that you take, you get suggestions on what your ideal next step should be. DataPrep can automatically detect schemas, data types, and anomalies.

**Watson StudioIBM Data Refinery**, available via IBM Watson Studio or Cloud Pak for Data, allows you to discover, cleanse, and transform data with built-in operations. It transforms large amounts of raw data into consumable, quality information that’s ready for analytics. Data Refinery offers the flexibility of exploring data residing in a spectrum of data sources. It detects data types and classifications automatically and also enforces applicable data governance policies automatically.

**Trifacta Wrangler** is an interactive cloud-based service for cleaning and transforming data. It takes messy, real-world data and cleans and rearranges it into data tables, which can then be exported to Excel, Tableau, and R. It is known for its collaboration features, allowing multiple team members to work simultaneously.

**Python** has a huge library and set of packages that offer powerful data manipulation capabilities. Let’s look at a few of these libraries and packages. **Jupyter Notebook** is an open-source web application widely used for data cleaning and transformation, statistical modeling, also data visualization. **Numpy, or Numerical Python**, is the most basic package that Python offers. It is fast, versatile, interoperable, and easy to use. It provides support for large, multi-dimensional arrays and matrices, and high-level mathematical functions to operate on these arrays. **Pandas** is designed for fast and easy data analysis operations. It allows complex operations such as merging, joining, and transforming huge chunks of data, performed using simple, single-line commands. Using Pandas, you can prevent common errors that result from misaligned data coming in from different sources.

**R**, too, offers a series of libraries and packages that are explicitly created for wrangling messy data—such as **Dplyr, Data.table, and Jsonlite**. Using these libraries, you can investigate, manipulate, and analyze data. **Dplyr** is a powerful library for data wrangling. It has a precise and straightforward syntax. **Data.table** helps to aggregate large data sets quickly. **Jsonlite** is a robust JSON parsing tool, great for interacting with web APIs.