Data transfer and storage formats

Name

Institution Affiliation

Data transfer and storage formats

Data transfer format

A database has many files and can be located in several places, and there are several formats of transferring these formats. HTTPS file transfer is the most used method for securing transactions online (Paxson, V. (2017, February). This file transfer gives us an illustration of combined secure protocol and hypertext transfer protocol, and its main function is to send data over unsecured networks, like the internet. HTTP operates at the topmost level of the TCP/IP model that formatting and sending data. SSL secures the connection used to send the data and works on a level lower of TCP/IP model. When the connection between the browser and the client is encrypted using a secure protocol, the URL of the connection will begin with HTTPS. HTTPS creates a secure connection by facilitating an encrypted link between any two systems like the server and the browser.

There are various advantages of https examples: secure communication because https ensures that the connection between the server and the browser is secure by encrypting the link. Https enhances data integrity because when data is encrypted, hackers cannot modify or read it even if they are successful in trapping the data. There is security and privacy with https because hackers cannot access any communication between the server and the browser (Kasneci, E. (2018). Faster performance is noted with https because it increases data transfer speed by reducing data size and encrypting the data. Using https also increases the ranking of SEO, but without https, Google shows a label of not secure in the browser. Https gives us a good representation of the future in the web by securing the internet and making it safe for owners of websites and users. Https is also reliable and facilitates verification of connections to determine if it is secure or insecure.

Some of the disadvantages of https are; it is costly, encrypting data needs many computations, there will be a challenge of caching in some contents, and there can be a confusion or configuration problem, thus downloading insecure contents from HTTP instead of https.

Data storage format

When data is in software, it should be stored for future use, and it is usually stored in storage systems of the software. When needed, the files or documents can be restored, and in this case, the storage system will need the assistance of other media (Nikulchev, E. (2021). With data storage, data recovery is quick, and backup is facilitated in a cyber-attack; the data will be safe. Data can be stored in disk drives, physical hard drives, virtually in the cloud, or in USB drives, and due to their reliability, a user can find data easily if the system crashes. ASCII is a format for storing data, and it converts information to digital formats that are standardized to allow effective communication of computers to enable processing and data storage. The advantage of ASCII is that it stores all alphanumeric characters because it uses the English language, ASCII uses less space, and there is no worrying of less space when using this code for storage; this is because it only has 256 characters.

The ASCII advantage of using the English language can also be a disadvantage because anyone who does not understand English cannot use it. If another code is used to write a document, the ASCII code will not read the document; instead, it will display certain characters and not the entire content. ASCII is a commonly used format for text files on the internet and computers (Nikulchev, E. (2021). ASCII files are standardized, which facilitates the importation of files into a different program from the origination program of the file. Files in ASCII can be useful in batch files like logon script and several others. Files in ASCII contain unformatted texts, and it means that any platform can read and understand the files.

Reference

Belov, V., Tatarintsev, A., & Nikulchev, E. (2021). Comparative Characteristics of Big Data Storage Formats. In *Journal of Physics: Conference Series* (Vol. 1727, No. 1, p. 012005). IOP Publishing.

Durumeric, Z., Ma, Z., Springall, D., Barnes, R., Sullivan, N., Bursztein, E. ... & Paxson, V. (2017, February). The Security Impact of HTTPS Interception. In *NDSS*.

Fuhl, W., Kuebler, T., Brinkmann, H., Rosenberg, R., Rosenstiel, W., & Kasneci, E. (2018). Link to data: https://atreus. informatik. uni-tuebingen. De/seafile/d/8e2ab8c3fdd444e1a135/? p=% 2FEyetrace&mode= list.