SEC-101: Data and Information Fundamental Assessment

Name: Thanawin Pattanaphol
Nickname: Win
Email: tpattan@cmkl.ac.th

Selected AI System Name: YouTube Recommendation System

System Description:

The YouTube recommendation system is a deep neural network, a type of machine learning model, that as YouTube defines it, “helping people find the videos they want to watch and that will give them value”. The YouTube recommendation system can be found on the homepage and the “Up Next” panel. It is “a mixture of personalized recommendations, subscriptions, and the latest news and information” [1].

The scope of the YouTube recommendation system includes video recommendation on the front page and the “Up Next” section below the video that the user is currently watching – the data of the recommendation system is collected from user engagements on the platform across their signed-in devices, such as: clicks, watch time, survey responses, sharing, likes, and dislikes. [1]

YouTube’s main goal is to provide users with new, personalized, and interesting content for each user, while also reducing the amount of video content, called “borderline content”, that contains inaccurate, misleading, deceptive, insensitive, intolerant or harmful content or information to below 0.5% of overall views on the platform.

List of Data and Information Required for the Selected AI System:

Table of Data used in YouTube’s video recommendation system.

Name	**Description**	**Type**	**Example**	**Sensitivity**	**Justification**
User ID	Unique identifier of a user	String	“UCiMhD4jzUqG-IgPzUmmytRQ”	Low	A useful string that can be used to track user interactions while being able to maintain the anonymity of the user.
Name	Display of the name user	String	“Beam”	Low	Usually public, therefore, it is not highly sensitive.
Age	Age of the user	Integer	19, 25, 38	Moderate	To some, age is considered as private as it can be risky to be

					revealed in public.
Gender	Gender of the user	String	“Men”	Low	Gender cannot be used to identify an individual.
Language Preference	The language that the user prefers	String	“English”	Low	Languages are not highly sensitive and is usually public.
Location	The location of where the user is watching from	String	“Bangkok, Thailand”	High	Locations can reveal private information and the user’s location data.
Video Title	Title of the video watched	String	“La Casa De Papel - Bella Ciao [Lyrics] (Money Heist) ”	Low	Video titles are usually public.
Video Description	Description content of the video watched	String	“La Casa De Papel - Bella Ciao [Lyrics] (Money Heist) Popular song from famous Netflix series La Casa De Papel (Money Heist)”	Low	Video descriptions are usually public.

Video Tags	Tags of the video watched	JSON/ Array	{
			“bella ciao”,
			“video”
			}
				Low	Video tags are usually public.

Watch History	List of videos that were watched by the user	JSON/ Array	{
			“OtFu51V_atA”,
			“_EWVsNHI4Hc”
			}
				High	This data reveals the user’s past preferences

Search History	List of search queries made by the user	JSON/ Array	{
			“how to write essay”,
			“latest news in Gaza”
			}
				High	Reveals the user’s preference, interests and intents.

Channel Subscriptions	List of YouTube channels that the user	JSON/ Array	{ “@TheMajorityReport”, “@cnn”, “@wsj”	High	Reveals the user’s preference on their content.

	subscribes		}		

Likes	List of videos that the user liked	JSON/ Array	{
			"HWl3YA3EEl4",
			"MP4FCxWnxSw",
			"wYS70hxsPME"
			}
				High	Reveals the user's preference, positive,

Dislikes	List of videos the user disliked	JSON/ Array	{
			"5zQ0WewZY50",
			"Sg-h4jpXsPI",
			"rdBF5seCfwg"
			}
				High	Reveals the user's preferences, negative opinions.

"Not Interested" Feedback	List of videos the user labeled as "Not interested"	JSON/ Array	{
			"CpiFXrQodP0",
			"Px9qhDGv300"
			}
				High	Reveals the user's intentions on certain videos.

Clicks	List of videos the user clicked on	JSON/ Array	{
			"hd63gAg26s5",
			"aJH4A_5Acd"
			}
				High	Reveals the user's interactions with videos.

Watchtime	The amount of time spent on videos	Integer	500	High	Reveals potential information regarding the user's interests.
Sharing	If the user shares a video or not	Boolean	false	Moderate	Can be used to identify personal choices.

Data Acquisition and Preprocessing Methods:

Step 1: Business Problem

YouTube's business problem is to provide users with content that they are interested in without the inclusion of "borderline content" or content that is considered misleading or inaccurate content for users.

YouTube's goal is to develop a recommendation system that uses past data, such as, the user's viewing history, search history, and other metrics.

Step 2: Data Acquisition

Input	Output
Raw user data (watch history, search queries, likes/dislikes, and other engagement numbers)	Large-scale datasets stored in YouTube's database.

Sources of Data Collection:

YouTube collections user metadata to understand content preferences, they are metadata properties, such as:

- Watch history - What each user have watched and how long they have watched the video (watch time).
- Search History – What the user searched on the platform.
- Account Metadata – The user's metadata, such as, age, gender, location, and others.
- Content Metadata – The metadata of the videos the user watched.

Step 3: Data Preparation

YouTube must clean and remove any data that contains duplicates, missing values, or any data that is not needed for the model; along with re-structuring the data, turning the dataset into a more organized, clean, and clearer dataset for the model.

Input	Output
Unfiltered dataset with possibly duplicates and missing values.	Structured, cleaned dataset to be used by the recommendation model.

Step 4: Exploratory Data Analysis

Input	Output
Cleaned dataset	Summary of behavioral and content trends.

Example of selected features that can be used for exploratory data analysis.

User ID	**Age**	**Language Preference**	**Watch History**	**Search History**	**Channel Subscriptions**	**Likes**	**Dislikes**
UCC4vs_6IdURyXrwYa74k-jw	28	"English"	{ "HWl3YA3EEl4", "MP4FCxWnxSw",	{ "Computers", "Laptop", "Phones" }	{ "@TheMajorityReport", "@cnn", "@wsj" }	{ "cxa1Y71Lgyg", "p8eiCJVK0M4",	{ "O7RJMQEPx5g" }

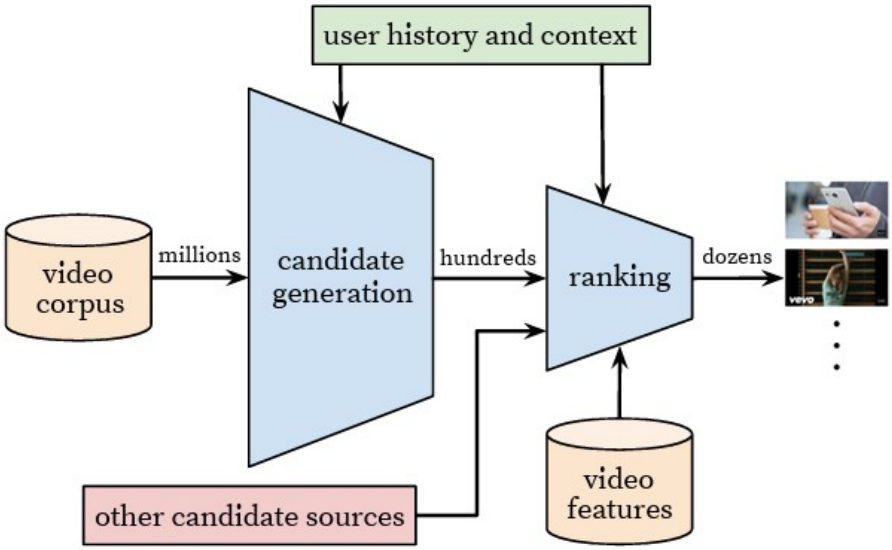
			“wYS70hxsPME” }			“wYS70hxsPME” }	

UC0vAgKbULmmOPCho39oBFvQ	30	“Thai”	{
			“5zQ0WewZY50”,
			“Sg-h4jpXsPI”,
			“rdBF5seCfwg”
			}
				{
				“วิธีผัดข้าว”.
				“ทาทา ยัง เพลง”,
				}
					{
					“@TV3HD”,
					“@ThairathTV”,
					“@ThaiPBS”
					}
						{
						“ycVLlIHTkpI”,
						“SIEmF568kAo”
						}
							{
							“W8AzNAekDrk”
							}

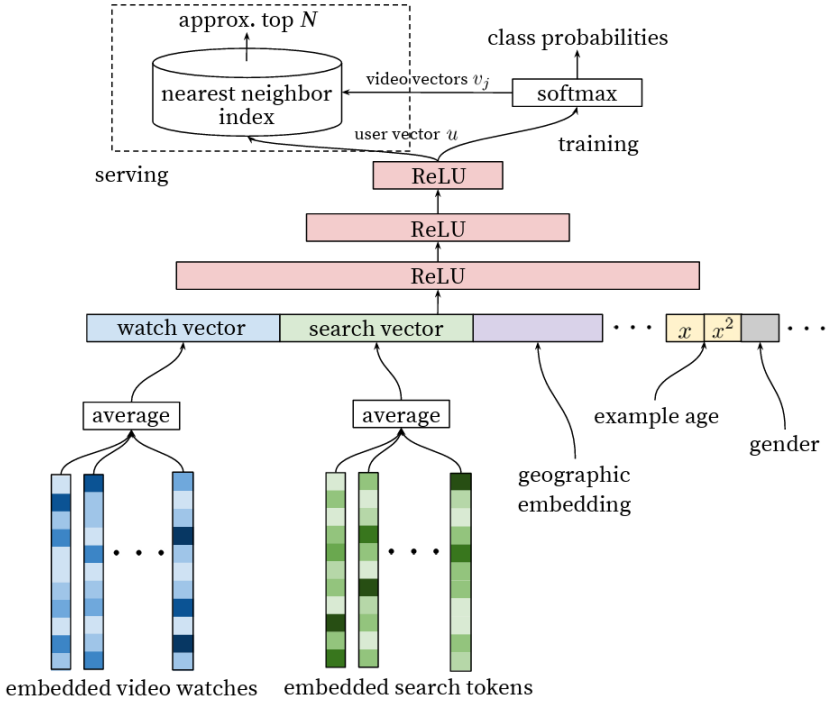
UC0XZoZMzvU_h4tObzN-22Ng	40	“Mandarin”	{
			“OtFu51V_atA”,
			“_EWVsNHI4Hc”
			}
				{
				“中華民國”,
				“我愛你”,
				“喜歡吃飯”
				}
					{
					“@CGTN”,
					“@CCTV”,
					“@ChinaNews”
					}
						{
						“CpCtY0JQvjs”,
						“at-smySDPNU”,
						“CPiFXrQodP0”
						}
							{
							“4N1iwQxiHrs”,
							“j32Z_el1uqk”
							}

Step 5: Data Modeling

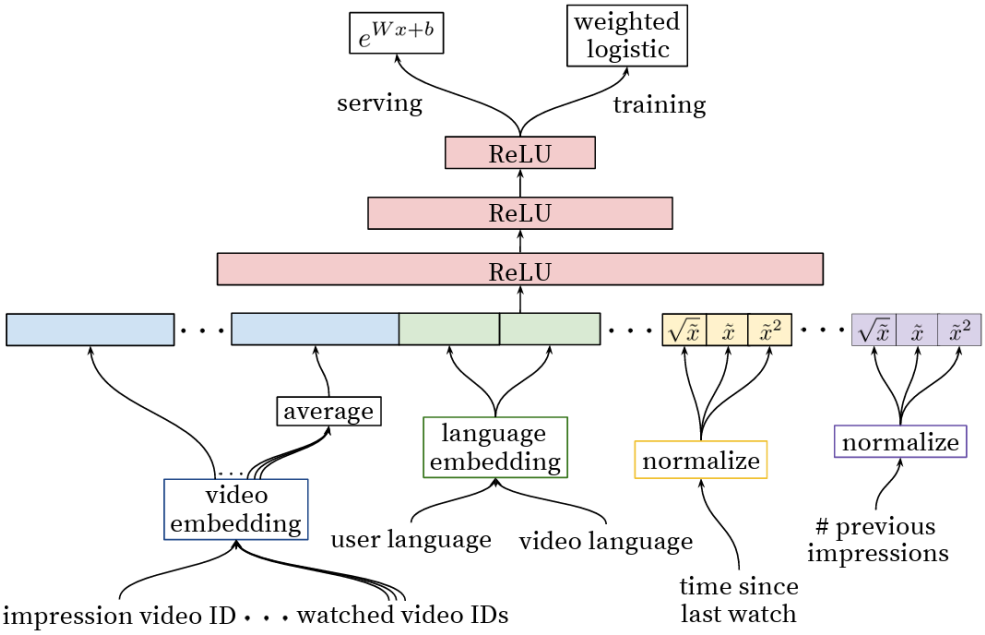
Overall – YouTube uses two neural networks for candidate generation and ranking: candidate generation & ranking.



Candidate generation – This network's goal is to filter out several thousand videos from the vast amount of data (usually called: corpus) based on user watch history, leaving with data that are relevant to the user. It uses features such as video Ids, demographics and search queries to generate the candidates.

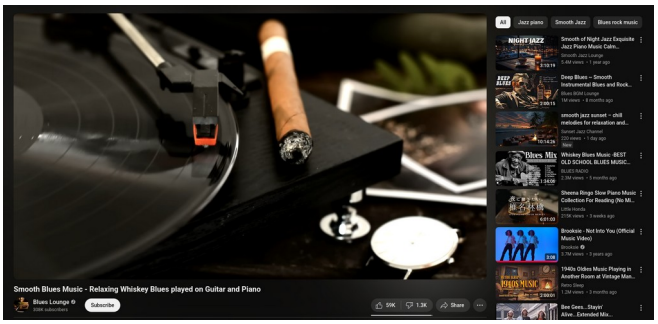


Ranking – This network essentially takes video candidates generated by the candidate generator and ranks them in order of their relevance to the user. Due to this, the network uses more “parameters” or “features” from both the video metadata and user metadata.

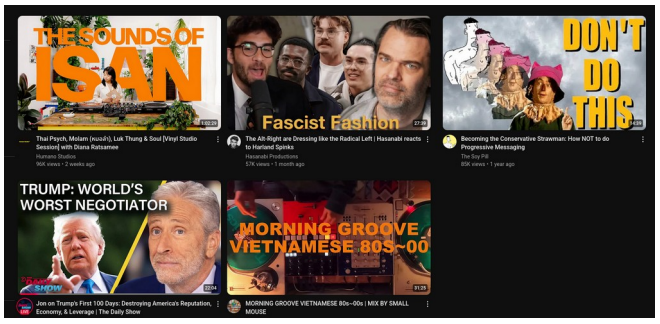


Step 6: Deploy & Maintenance

YouTube integrates the recommendation model to the platform, users are now able to see their personalized suggestions on the homepage and “Up Next” tab.



“Up Next” section on the right side



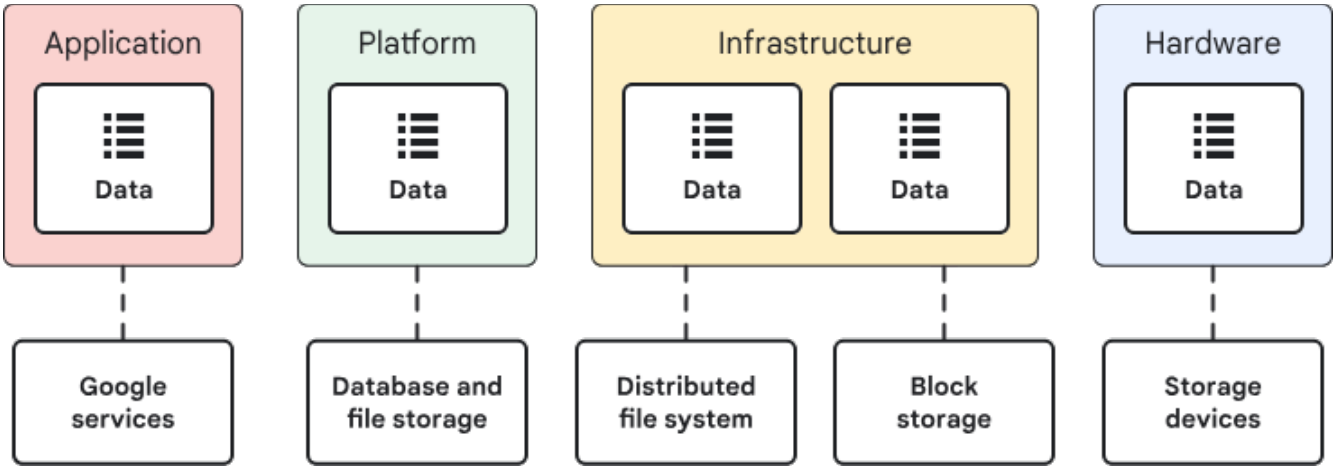
Homepage recommendation section

However, due to the fact that YouTube’s recommendation system is a personalized system, the model would still need to have new data fed in to adjust the video recommendation output according to the new data that is fed to it. Thus, YouTube still needs to collect user’s watch history and other metrics, along with regularly implement data security measures and updates to protect privacy.

Security Analysis of the Data and Information:

YouTube's enormous dataset contains high-sensitivity data attributes, such as, search histories, location data, subscription list – due to the properties of these attributes being able to potentially reveal personal preferences, biases, habits, location, and identity; and low sensitivity data attributes, such as, names, gender, and other attributes. Due to this fact, YouTube has included security guidelines to protect any private information related to the user, such as, the use of encryption. Encryption is specifically used for search histories, and other sensitive data – according to Google Cloud [3], Google, YouTube's parent company, uses the standard Advanced Encryption Standard (AES) algorithm: AES-256; along with the cryptographic library, "Tink", which uses Google's FIPS 140-2 validated module named "BoringCrypto".

Google uses the "encrypted at rest" concept where, as Google specifies in its documentation: "encrypts all customer content stored at rest, without any action from the user, using one of more encryption mechanisms." [3]. Google also uses layers of encryption to help protect data, in which, they use different mechanisms for different aspects of the Google Cloud infrastructure as outlined below.



For example, Google's encryption at the infrastructure layer divides up data into several chunks, they are then encrypted at the storage level with individual data encryption keys. Google encrypts data before writing it to a database storage system or hardware disk. Google also uses Access control lists (ACLs) to help ensure that each chunk can be decrypted only by Google services that accessible to specific data storage places.

Google's data and information encryption level is indeed at a very secure level, however, it is still recommended to either, reduce as much personal or sensitive data collection as much as possible – due to the possibility of data leaks, or, use data anonymization techniques to reduce the chances of leaked data being able to be used to identify a user.

Privacy Analysis of the Data and Information:

Google's dataset contains a significant amount of personal data attributes, such as, user Ids, name, age, watch history, search history, location data, and other attributes that can be used to reveal personal

interests, watch habits, and potentially physical locations – this could lead to re-identification of the user if the data is then used with another dataset that contains the same user data.

However, Google as done a good job at securing their users' / customers' personal or sensitive data through the security measures taken by Google as mentioned in the section above. Although, it is still recommended that Google should give the users a choice when it comes to data collection as some people might not demand a personalized video recommendation or having their data being collected. Therefore, Google should give the user a way to opt-out of their data collection services, as well as being more transparent when it comes to data collection; this also helps Google in complying with data privacy regulations, such as, the GDPR, CCPA, or PDPA.

References:
[1] https://blog.youtube/inside-youtube/on-youtubes-recommendation-system/
[2] https://dl.acm.org/doi/10.1145/2959100.2959190
[3] https://cloud.google.com/docs/security/encryption/default-encryption