

Theory 2

	Web 1.0	Web 2.0	Web 3.0	Web 4.0	Web 5.0
Time Period	Around 1990 to 2000	Stayed during 2000 - 2010	Approx . 2010-2020	It is the present technology that started from 2020	Still need to be implemented
Content Type	Static content :Read Only web and Static HTML pages	Dynamic Content: User interaction data such as like comments etc	Semantic Content: Personalized content	Currently running technology such as integrated devices and context aware services.	Emotional Content such as emotionally interactive and humanized interfaces
User Interaction	Limited Interaction with passive consumption and basic hyperlinks and forms	Increased Interaction such as social networking and content sharing	Intelligent Interaction i.e. we will get the content based on the personal behavior	Seamless interaction , across multiple devices and IoT integration	Symbiotic Interaction such human-computer convergence and emotional and cognitive interfaces
Technology used	Foundational technology such as html , basic css and simple web servers.	Interactive technology such as JavaScript , AJAX, XML and RSS feeds.	Intelligent Technologies such as Semantic web i.e. RDF, OWL. One more is AI and machine learning	Such as Internet of Things and cloud computing and advanced AI	Futuristic Technologies - Affective computing - Neural interfaces - Advanced artificial intelligence
Example Platforms	Most of the early websites such persona homepages	Most of the social media platforms	Smart Assistant such as Siri, Google	Connected Ecosystems - Smart homes	Emotional AI Systems - Brain-computer

	and static company sites	such as Facebook, YouTube etc	Assistant ,Personal web services etc.	- Wearable devices - Autonomous vehicles	interfaces - Emotion-recognition applications
Security Concerns	Threats such as lack of encryption as there was no https and server vulnerabilities.	There is data privacy risk such as identify theft i.e. one can mimic as the other user to perform social engineering attack. One more is unauthorized data sharing.	There are huge violations in data privacy such as data mining abuse and surveillance concerns such as unwanted data capture from users etc.	IoT Vulnerabilities such as device hacking and large-scale data breaches	Ethical and Privacy Issues - Emotional data exploitation - Manipulation of thoughts and behaviors
Possible Attacks	Simple defacement, directory traversal i.e. directory enumeration.	Main exploits are Phishing scam, along with high skill attack such as Cross site scripting and sql injection.	Attacks are advanced here such as semantic attacks and advanced persistent threats.	Attacks are complex in nature and since many devices are involved lead to the creation of botnets which help in achieving DDOS. And lots of devices are connected, there may one device that is highly vulnerable may lead to entry point to different devices.	Psychological Attacks - Deepfakes - Emotional manipulation - Cyber-psychological warfare