



# CTC(T&IT), CRPF



Monthly

# e-Newsletter

March - 2022



Never stop learning, Because life never stop Teaching

**“I am the master of my failure...  
If I never fail how will I ever learn..”**

**— C.V RAMAN**

**MAR-2022, Published on Mar-31-2022**

## **EDITOR'S CENTER**

*Patron*

**Sh. Harjinder Singh, DIGP  
Principal CTC(T&IT)**

*Editor & Publisher*

**Sh.Shitole Dhiraj Gorak, AC**

*Editorial Assistance*

**Insp/T Harish Prasad**

*Designing & Photography*

**HC/RO P.Albin**



**Published By  
CTC(T&IT),CRPF,Ranchi**

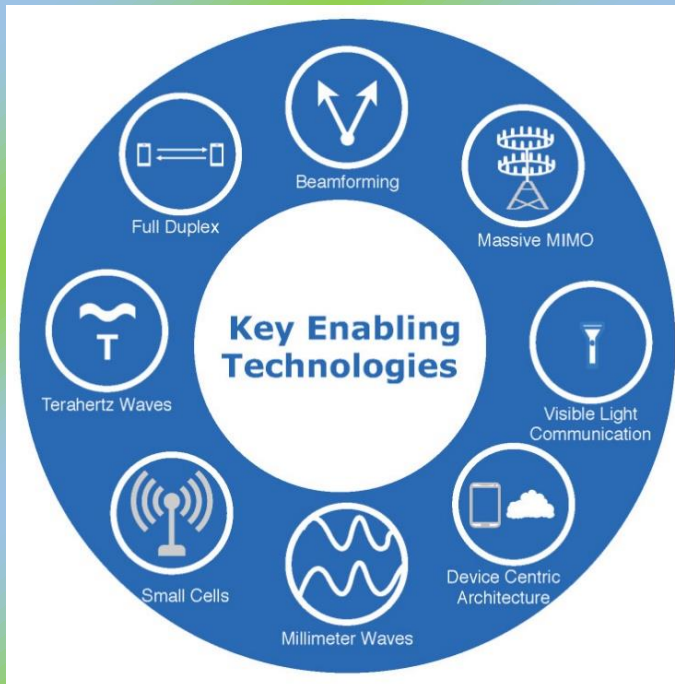
## **READER'S CENTER**

- 1. Technological Advancements in 5G**
- 2. Android Automotive**
- 3. Brain Computer Interface Technology**
- 4. Hash Function**
- 5. Quiz Corner**



# Technological advancements in 5G

5G is the 5th generation mobile network. It is a new global wireless standard after 1G, 2G, 3G, and 4G networks. 5G enables a new kind of network that is designed to connect virtually everyone and everything together including machines, objects, and devices.



5G will bring wider bandwidths by expanding the usage of spectrum resources, from sub-3 GHz used in 4G to 100 GHz and beyond. 5G can operate in both lower bands (e.g., sub-6 GHz) as well as mmWave (e.g., 24 GHz and up), which will bring extreme capacity, multi-Gbps throughput, and low latency.

5G is based on NOMA (NON Orthogonal frequency-division multiplexing), a method of modulating a digital signal across several different channels to reduce interference.

5G uses 5G NR air interface alongside OFDM principles. 5G uses Massive MIMO Antenna systems with beamforming. 5G uses 256 QAM modulation technique.

Other enhancing factors are virtual network, Multi-Access Edge Computing (MEC), Network function virtualization (NFV), O-RAN, edge computing

5G is designed to not only deliver faster, better mobile broadband services compared to 4G LTE, but can also expand into new service areas such as mission-critical communications and connecting the massive IoT. This is enabled by many new 5G NR air interface design techniques, such as a new self-contained TDD subframe design.

With high speeds, superior reliability and negligible latency, 5G will expand the mobile ecosystem into new realms. 5G will impact every industry, making safer transportation, remote healthcare, precision agriculture, digitized logistics — and more — a reality

Sh. Shitole Dhiraj Gorak, Asstt. Comdt.

# Android Automotive

Android Automotive is a base Android platform that runs pre-installed IVI system Android applications as well as optional second- and third-party Android Applications.

Android Automotive offers openness, customization, and scale to automotive infotainment systems and head units. Openness enables new efficiencies by providing basic automotive infotainment features in a free and open source codebase. Customization enables implementers to differentiate the product as they see fit. Scale is achieved through Android's common framework, language, and APIs, all of which enables reuse of development expertise and completed software from hundreds of thousands of Android developers worldwide.

## Android Automotive & Android

It's important to understand how Android Automotive relates to the overall Android ecosystem:

**Android Automotive is Android.** Android Automotive is not a fork or parallel development of Android. It is the same codebase and lives in the same repository as the Android shipped on phones, tablets, etc. It builds on a robust platform and feature set developed over 10+ years, enabling it to leverage the existing security model, compatibility program, developer tools, and infrastructure while continuing to be highly customizable and portable, completely free, and open source.

**Android Automotive extends Android.** In the course of building Android into a full-featured platform for infotainment, we're adding support for automotive-specific requirements, features, and technologies. Android Automotive will be a full-stack, turnkey automotive infotainment platform, just as Android is for mobile today.

Carriers, OEMs, and developers have been using Android to build beautiful devices, applications, and experiences for over a decade. Android Automotive now brings the power of Android to the car, where car makers can create powerful infotainment systems designed for the digital age.

## Android Automotive & Android Auto

The nomenclature can be confusing. Here's how they differ:

**Android Auto is a platform running on the user's phone,** projecting the Android Auto user experience to a compatible in-vehicle infotainment system over a USB connection. Android Auto supports apps designed for in-vehicle use.

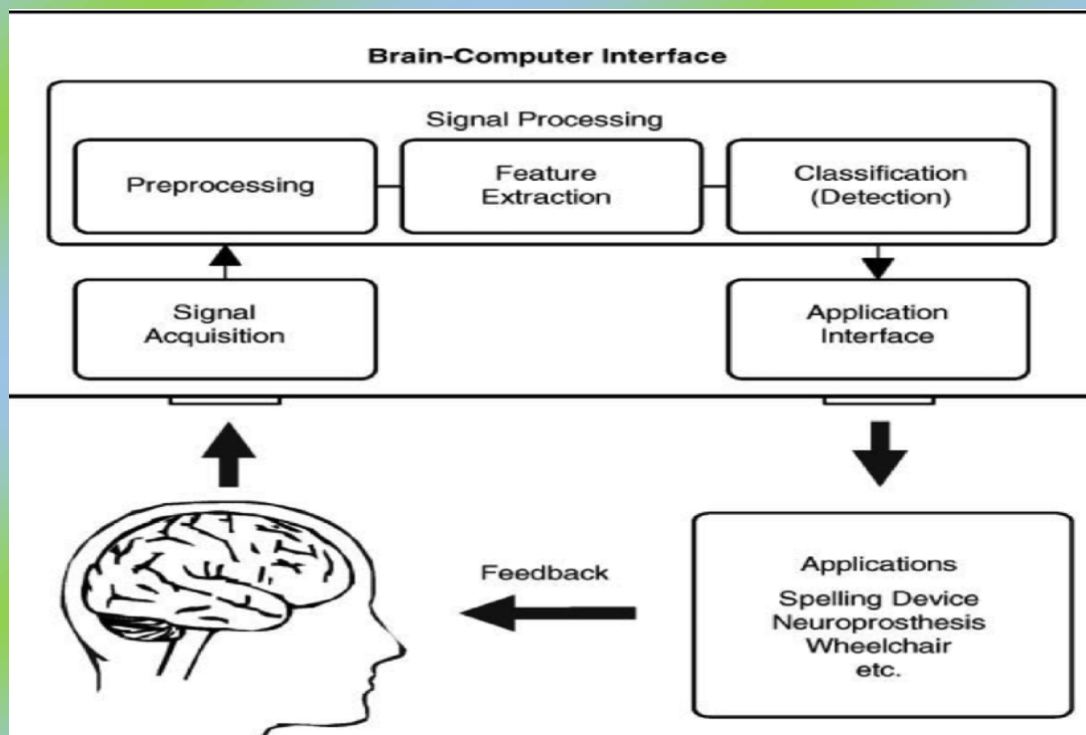
**Android Automotive** is an operating system and platform running directly on the in-vehicle hardware. It is a full-stack, open source, highly customizable platform powering the infotainment experience. Android Automotive supports apps built for Android as well as those built for Android Auto.

## **Google Automotive Services (GAS)**

Google Automotive Services (GAS) is a collection of applications and services that automotive OEMs can choose to license and integrate into their in-vehicle infotainment (IVI) systems. For details and access to latest version of GAS applications, reach out to your Google point of contact.

HC/RO Satender Singh Suhag

# **BRAIN COMPUTER INTERFACE TECHNOLOGY**



Brain computer interface is one of the most promising and increasingly popular technologies for assisting and improving communication/control for motor paralysis (e.g., paraplegia or quadriplegia) due to stroke, spinal cord injury, cerebral palsy, and amyotrophic lateral sclerosis (ALS). Eye-tracking technology also allows paralyzed people to control external devices but it has many drawbacks due to the way of measuring the eye movements via cameras or using attached electrode on face such as electrooculography (EOG) signals. BCI essentially involves translating human brain activity into external action by sending neural commands to external devices. Although, the most common use of BCI is to help

disabled people with disorders in the motor system, it might be very useful tool for improving the quality of life of healthy people, particularly the elderly. Assistive, adaptive, and rehabilitative BCI applications for older adults and elderly patients should be developed to assist with their domestic chores, enhance relationships with their families and improve their cognitive and motor abilities. BCI technology has clinical and non-clinical applications in many areas, including medicine, entertainment, education, and psychology to solve many health issues such as cognitive deficits, slowness in processing speed, impaired memory and movement capability decline among elderly people. These issues can affect the quality of elderly life and may have adverse effects on mental health. To help older people maintain a healthy, good quality of life and sense of wellbeing, many BCI applications have been developed in the past decade.

There are two types of BCI based on the electrodes used for measuring the brain activity: non-invasive BCI where the electrodes are placed on the scalp (e.g., EEG based BCI), and invasive Brain computer interface where the electrodes are directly attached on human brain [e.g., BCI based on electrocorticography (ECoG), or intracranial electroencephalography (iEEG)].

Brain computer interfaces using EEG technology have been widely used to establish portable synchronous and asynchronous control and communication. Non-invasive EEG-based BCIs can be classified as “evoked” or “spontaneous.” An evoked BCI exploits a strong characteristic of the EEG, the so-called evoked potential, which reflects the immediate automatic responses of the brain to some external stimuli. Spontaneous BCIs are based on the analysis of EEG phenomena associated with various aspects of brain function related to mental tasks carried out by the BCI user at their own will. These BCIs have been developed based on some brain features such as evoked potentials [e.g., P300 and steady-state visual evoked potential (SSVEP)] or based on slow potential shifts and variations of rhythmic activity [e.g., motor imagery (MI)].

One of the greatest challenges in BCI technology is the development of less invasive or non-invasive technologies for paralyzed patients. Using non-invasive devices can greatly reduce the both the total cost of surgical operation and the physical harm to the patient. However, non-invasive methods can lead to weaker signals and a low signal-to-noise ratio (SNR) with less source precision and lower spatial resolution. These drawbacks can be partially overcome with advanced methods such as deep learning to decode and extract more relevant source information from the EEG signal

Electroencephalogram -based BCI technology has many important applications in the medical and psychology fields not only for motor control impairments. One promising application for elderly patients is the development of automatic systems to detect the influences on the brain signal related the smoking and alcohol abuse using resting-state EEG). BCI has also been found to be helpful in identifying deficits and improving social skills in patients with autism through the use of BCI-assisted social games. Other research has focused on systems to test memory capacity and cognitive level.

HC/RO B.Venkatesan

# HASH FUNCTION

Hashing is an algorithm that calculates a fixed-size bit string value from a file. A file basically contains blocks of data. Hashing transforms this data into a far shorter fixed-length value or key which represents the original string. The hash value can be considered the distilled summary of everything within that file.

A good hashing algorithm would exhibit a property called the avalanche effect, where the resulting hash output would change significantly or entirely even when a single bit or byte of data within a file is changed. A hash function that does not do this is considered to have poor randomization, which would be easy to break by hackers.

A hash is usually a hexadecimal string of several characters. Hashing is also a unidirectional process so you can never work backwards to get back the original data.

A good hash algorithm should be complex enough such that it does not produce the same hash value from two different inputs. If it does, this is known as a hash collision. A hash algorithm can only be considered good and acceptable if it can offer a very low chance of collision.

## What are the benefits of Hashing?

One main use of hashing is to compare two files for equality. Without opening two documents/files to compare them word-for-word, the calculated hash values of these files will allow the owner to know immediately if they are different.

Hashing is also used to verify the integrity of a file after it has been transferred from one place to another, typically in a file backup program like syncBack. To ensure the transferred file is not corrupted, as user can compare the hash value of both files. If they are the same, then the transferred file is an identical copy.

In some situations, an encrypted file may be designed to never change the file size nor the last modification date and time (for example, virtual drive container files). In such cases, it would be impossible to tell at a glance if two similar files are different or not, but the hash values would easily tell these files apart if they are different.

## Types of Hashing

There are many different types of hash algorithms such as RIPEMD, Tiger, xxhash and more, but the most common type of hashing used for file integrity checks are MD5, SHA-2 and CRC32. MD5-An MD5 hash function encodes a string of information and encodes it into a 128-bit fingerprint. MD5 is often used as a checksum to verify data integrity. However, due to its age, MD5 is also known to suffer from extensive hash collision vulnerabilities, but it's still one of the most widely used algorithms in the world.

SHA-2-SHA-2, developed by the National security agency(NSA), is a cryptographic hash function. SHA-2 includes significant changes from its predecessor, SHA-1. The SHA-2 family

consists of six hash functions with digests (hash values) that are 224,256,384,or 512 bits: SHA-224,SHA-256,SHA-384,SHA-512,SHA-512/224,SHA-512/256

**CRC32-** A cyclic redundancy check (CRC) is an error-detecting code often used for detection of accidental changes to data. Encoding the same data string using CRC32 will always result in the same hash output, thus CRC32 is sometimes used as a hash algorithm for file integrity checks. These days,CRC32 is rarely used outside of Zip files and FTP servers.

**RipeMD-RipeMD** (RIPE Message Digest) is a family of cryptographic hash functions developed in 1992 (the original RIPEMD) and 1996(other variants).There are five functions in the family:RIPEMD,RIPEMD-128,RIPEMD-160,RIPEMD-256 and RIPEMD-320,of which RIPEMD-160 is the most common. The original RIPEMD, as well as RIPEMD-128,is not considered secure because 128-bit result is too small and also (for the original RIPEMD) because of design weaknesses. The 256-and 320-bit versions of RIPEMD provide the same level of security as RIPEMD-128 and RIPEMD-160,respectively; they are designed for applications where the security level is sufficient but longer hash result is necessary.

**Tiger-**In cryptography, Tiger is a cryptographic hash function designed by Ross Anderson and Eli Biham in 1995 for efficiency on 64-bit platforms. The size of a Tiger hash value is 192 bits. Truncated versions (known as Tiger/128 and Tiger/160) can be used for compatibility with protocols assuming a particular hash size. Unlike the SHA-2 family, no distinguishing initializations values are defined; they are simply prefixes of the full Tiger

**Using Hashing in 2BrightSparks software** In the backup and synchronization software , SyncBackPro /SE. Free hashing is mainly used for file integrity checks during or after a data transfer session. For example, a Sync Back user can turn on file verification (Modify profile> Copy/delete) or use a slower but more reliable method (Modify profile>Compare options) which will enable hashing to check for file differences.

Different hash functions will be used depending on which option is used and where the backup files are located. Other areas where hashing is used are resuming in FTP, data integrity checking , scripting and occasionally for authentication in cloud profiles (scripting and cloud backup is supported by SyncBackPro only).

2Bright sparks also has a utility program called hash on click that can be used to ensure files are identical. Hash on click is part of on click utilities, which is completely free. several types of hashing algorithms are available in Hash on click.

HC/RO Rohit

# QUIZ

**1. A software that allows a personal computer to pretend it, as a terminal is**

- (A) Terminal emulation
- (B) Modem
- (C) Bulletin board
- (D) Auto-dialing

**2. Which of the following techniques is used for Time-To-Line (TTL)?**

- (A) A technique used to best-effort delivery systems to avoid endlessly looping packets.
- (B) A technique used by protocols in which a lower level protocol accepts a message from a higher level protocol and places it in the data portion of the low level frame.
- (C) One of the pieces that results when an IP gateway divides an IP datagram into smaller pieces for transmission across a network that cannot handle the original datagram size.
- (D) All of these

**3. Which of the following TCP/IP protocol is used for the file transfer with minimal capability and minimal overhead?**

- (A) TFTP
- (B) TELNET
- (C) FTP
- (D) RARP

**4. Binary Coded Decimal (BCD) numbers express each decimal digit as**

- (A) Binary digits
- (B) Byte
- (C) Word
- (D) Nibble

**5. A station in a network forwards incoming packets by placing them on its shortest output queue. What routing algorithm is being used?**

- (A) Delta routing
- (B) Static routing
- (C) Flooding
- (D) Hot potato routing

**6. A facility that allows the user to speak into a special device while typing a letter using computer is called \_\_\_\_**

- (A) Speaker
- (B) Dictaphone
- (C) Telephone
- (D) Cell phone

**7. ITES stands for \_\_\_\_**

- (A) Information Technology Entrusted Systems
- (B) Information Technology Extended Services
- (C) Information Technology Enabled Services
- (D) Improving Technology Enlighted Services

**8.A turnkey package includes**

- (A) Training
- (B) Software
- (C) Hardware
- (D) All of these

**9. A channel for communicating across a boundary between two or more subsystem is known as**

- (A) Data path
- (B) Walk through
- (C) Act gram
- (D) Interface

**10. CGI stands for \_\_\_\_**

- (A) Common Gateway Internet
- (B) Common Gateway Interface
- (C) Central Gateway Interface
- (D) Central Gateway Internet

## Acknowledgement

We are highly thankful for reading out this compilation and hope it will be useful for you in day to day professional and personal life .We would like to hear your interest areas, suggestions from you to make this newsletter more informative and interesting. Your views will definitely help us to create this newsletter as an effective medium to reach you with latest development in the fields of communication and technology.

## R&D Team

CTC T&IT CRPF, Ranchi, Jharkhand  
ctcit@crpf.gov.in

### Answer key

|    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|
| 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 |
| A  | A  | A  | B  | D  | B  | C  | D  | D  | C  |