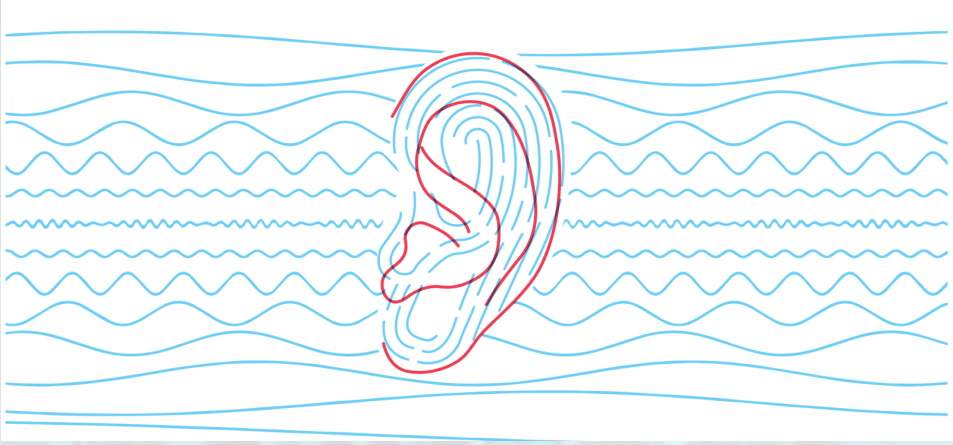
These systems operate with the user's knowledge and typically require their cooperation. For example, presenting a person's passport at border control is a verification process - the agent compares the person's face to the picture in the document.

VOICE - SPEAKER IDENTIFICATION: Identification is the task of determining an unknown speaker's identity. Speaker identification is a 1: N (many) match where the voice is compared against N templates. Speaker identification systems can also be implemented covertly without the user's knowledge to identify talkers in a discussion, alert automated systems of speaker changes, check if a user is already enrolled in a system, etc. For example, a police officer compares a sketch of an assailant against a database of previously documented criminals to find the closest match. In forensic applications, it is common to first perform a speaker identification process to create a list of "best matches" and then perform a series of verification processes to determine a conclusive match.



All the above techniques has some or the other drawbacks. With the new research and analysis an "Ear print" is considered to be a new way of biometric providing securities especially for mobile phones.

With the horrible unreliability in other recognition techniques, inspired the scientists from Descartes Biometrics to develop a new identification device – the Earprint.

It sends the sound in your ear which is then echoed back. This echo is different for every person. If you want to utilize Earprint, you've got to download special software on your phone. This software will then use the smartphone sensors to do its job. The process is quick and easy: you just need to press the touchscreen against your ear. So, this device might as well substitute fingerprints in the future. This latest technology invention can bring a new era for the cybersecurity world.


**Prof. Mohini Ghotekar**
**Assistant Professor**