**Article on "Forensic Basics of Machine 2 Brain Interface" and "AI on Digital Forensics”**

**Forensic Basics of Machine 2 Brain Interface**

A **Brain-Computer Interface** (BCI) is a computer-based system that acquires brain signals, analyzes them, and translates them into commands that are relayed to an output device to carry out a desired action. Thus, BCIs do not use the brain's normal output pathways of peripheral nerves and muscles. This definition strictly limits the term *BCI* to systems that measure and use signals produced by the central nervous system (CNS). An electroencephalogram (EEG) machine alone is not a BCI because it only records brain signals but does not generate an output that acts on the user's environment. It is a misconception that BCIs are mind-reading devices. Brain-computer interfaces do not read minds in the sense of extracting information from unsuspecting or unwilling users but enable users to act on the world by using brain signals rather than muscles. The user and the BCI work together. The user, often after a period of training, generates brain signals that encode intention, and the BCI, also after training, decodes the signals and translates them into commands to an output device that accomplishes the user's intention. A BCI, sometimes called a neural-control interface (NCI), mind-machine interface (MMI), direct neural interface (DNI), or brain-machine interface (BMI), is a direct communication pathway between an enhanced or wired brain and an external device. BCI differs from neuromodulation (*the alteration of nerve activity through targeted delivery of a stimulus, such as electrical stimulation or chemical agents, to specific neurological sites in the body*) in that it allows for bidirectional information flow. BCIs are often directed at researching, mapping, assisting, augmenting, or repairing human cognitive or sensory-motor functions. Recent studies in Human-computer interaction through the application of machine learning, EEG brainwave data has shown high levels of success in classifying mental states (Relaxed, Neutral, Concentrating) and mental emotional states (Negative, Neutral, Positive). In medical science, a neuroprosthetic is any device that can enhance the input or output of a neural system. It uses artificial devices to replace the function of impaired nervous systems and brain-related problems, or of sensory organs or organs itself (bladder, diaphragm, etc). Neuroprosthetics and BCIs seek to achieve the same aims, such as restoring sight, hearing, movement, ability to communicate, and even cognitive function.

Though there are many benefits of BCI such as Smart Technology (can help disabled people move their artificially replaced body parts easily), Telepresence (can allow military personnel to keep an eye on any suspicious activity taking place through a distance), Fewer Accidents (BCI-enabled car can help prevent accidents), etc. But they can have a negative impact on its users in case it is not utilized properly, as it’s directly linked to the human brain. Some major potential risk are as follows:

1. Inaccuracy of results: Sometimes we ourselves are unable to understand what goes on in our minds. So it is unfair to expect man-made BCI to correctly interpret all our brain signals. BCI can sometimes misinterpret the user’s intentions. Hence, the inaccurate result is a huge risk that is associated with the BCI technology.
2. Lack of Security: In the case of BCI technology, the security of your data cannot be guaranteed. Due to the computerized system, anyone may decode what is going on in your mind and thus invade your privacy. For instance, in the case of BCI based military applications, there might be a possibility that an attacker from a rival country will be able to hack into any military personnel's mind and can eventually leak all confidential information. Since the scientists have revealed that within the coming years attackers can potentially be able to rewrite memories in people’s minds.

**AI on Digital Forensics**

Artificial Intelligence (AI) refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions. The term may also be applied to any machine that exhibits traits associated with a human mind such as learning and problem-solving. On the other hand, Digital Forensics is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. Algorithms already play a significant role in helping digital forensics investigators analyze the vast amount of data that is created by mobile devices and stored on the clouds. Artificial Intelligence (AI) can help automate some processes and more quickly flag content or insights that would otherwise take investigators longer to uncover. It is a tool in the toolbox that is helping law enforcement agencies (and corporate in-house investigators) comb through the available data for insights—digital needles in the proverbial haystack. It can help with spotting and identifying elements in photos and videos, observing commonalities in communication, location, and times, and based on history, make educated guesses about where and when the next incident or crime might occur. There is a trust factor to overcome with AI in digital evidence in criminal investigations. When evidence in a case is presented, the attorneys, judges, and jury members must grasp the broad concept of artificial intelligence in order to accept and feel comfortable with it’s growing role in digital forensics and in many modern criminal investigations. Just human logic on complex decisions can be traced back and debated on any particular issue, it’s imperative that AI functions have logs and so its conclusions are transparent and can be fully litigated. An intelligent software agent (ISA) uses Artiﬁcial Intelligence (AI) in the pursuit of goals. Thus, an ISA interacts with the environment, perceiving and acting autonomously over it to achieve deﬁned goals. In an analogous way, a MultiAgent System (MAS) is a system where many agents interact with the environment in a cooperative or competitive way to achieve individual or group objectives. A multiagent system to assist the computer forensics expert on its examinations using MultiAgent Digital Investigation toolkit (MADIK). The system is composed of a set of ISAs that perform diﬀerent analysis on the digital evidence related to a case in a distributed manner. Identifying specific types or clusters of data in an investigation is best handled by a type of AI known as pattern recognition. The type of pattern recognition that people are most familiar with is perhaps image recognition, where the software attempts to identify parts of a picture. Other forms of pattern and image recognition also exist, such as detecting a pattern in ane-mail message which indicates SPAM, or a pattern in a disk image that might indicate it is part of a sound file.Many of the techniques used rely very heavily on statistics or probabilistic reasoning or both. The more complex and accurate forms of image recognition that might be used to locate certain types of picture, rely on an understanding of how the human perceptual system works. However, at present these have a high rate of false positives or false negatives (depending on where the thresholds are set) as well as being very computationally intensive. In the CBR system, a large collection of cases (and in digital forensics, the resultant actions) is obtained, and a metric is used to match the current situation with one found in the casebase. If a perfect match is found, then the action carried out in the initial case is applied to the existing situation.If no perfect match is found, but a match is found that is deemed to be close enough, then the system may attempt to adapt the action of the matched case to the current situation using what are called ‘repair’ rules.15CBR systems have the advantage of approaching a problem in a way that is familiar to the expert, can cope with large amounts of data, and can deal with situations that have not previously been encountered. The use of AI in digital forensics is still at a very early stage, but it does have a lot to offer the digital forensics community. In the short term it is likely that it can be immediately effective by the use of more complex pattern recognition and data mining techniques. However, for digital forensics to take full advantage of what AI has to offer, more work is necessary.