BCI Technology Ethically Misuse in the Society

DR: Nadeem ahmed[1]   Abrar Ahmed[2]   Aqeel Ahmed[3]   Ali Abbas[3]   Umair Latif[3]

nadeen.ahmad@superior.edu.pk |abrara980@gmail.com| braveaqeel@gmail.com| mianali.abbas1@gmail.com |umairgohar855@gmail.com

Department of CS and IT, Superior University Lahore [1]

Department of CS and IT, the University Of Lahore[2,3]

Abstract__ Brain control interface (BCI) technology is a device that controls the brain activities, its work with electroencephalogram (EEG) technology. BCI control the natural brain activities and simulate on computer interface. The basic purpose of BCI's device is medical treatment of mental sick person. BCI Technology used in medical, non-medical and military applications. It is use for treatment of different disease alike psychological problem and spinal cord injuries. BCI simulate the electron signal and data process device that is encode the subject's brain activities on BCI interface. BCI Technologies have some benefits and drawback. It is possible, its record the use privacy, history, social life, behavior and encode on computer Technology. Privacy included ATM PIN number, Email password, insurance policy information, Bank accounts information etc. BCI device connect to internet and may be subject's information to be public. In future may we will control all over activities of human alike thinking, feeling, personal life. We will be more interpreted other person life and performed anything we want to do, it is ethically immoral.

Keyword: brain hacking, ethically issues, social issue of BCI, Nauru-crime, privacy, brain cracking, security of BCI.

Introduction:

In [1], A Large number of Brain Computer Interface (BCIs) is being developed for different applications. In [3], the purpose of Brain Computer Interface (BCIs) devices is to get the neural information from the brain of users. In [21], BCI device encrypt the brain information and treat it. In [20], BCI technology translates user's instruction correctly into action according to user requirement. Brain Computer Interface (BCIs), Brain Natural computer interface (BNCI), and Nauru technology that used to control the devices with brain activity. BCI can record, stimulate and data processing system sometime we are called Brain Machine interface (BMI). These technologies are used to improve the control on human nerves, and treatment for Parkinson, disease and depression. BCI can also be controlled robotics devices. In [1], for example Samsung and university of Texas in May 2013 control mobile devices with BCIs. In [1], Nauru ware Company presented EEG System in September 2013 that is wearable device which is used to detect user emotions and get information through neural signals. In [4],[5],[6] Emotivea and Nauru Sky provides low price BCIs Development kits. These companies also introduced app stores for BCIs applications. USENIX in 2012 introduced the brain spyware application which is spiteful application that gets private information from the users like Pin Code, Credit Card Information, Date of Birth, and Location of Residence. There are numbers of benefits of BCI but some ethically risk also present in BCI like safety, privacy and

security and identification, neurons crime. In [2], this paper offers an overview of brain hacking and their ethical issues. Our aim is to provide the various aspect of brain hacking and their efficient treatment. We will proceed as follows:

Related Work:

Neurocrime:

In [3], Neurocrime technology direct access the brain and disturb the brain security. Our brain not only maintains life process but also maintain the other activity like thinking, movement, language, memory and our behavior. Therefore misuse of these neural devices for cybercrime damage the security of users. With Cybercrime technology we access the brain security indirect manner like limiting modifying or disrupting function in the devices that interface brain computation. Neurocime devices available in medical, non medical, commercial and military products these type of devices directly finish the function of product without any authorization. These types of criminal activity affect the human being of groups of human being with direct or indirect physical or mental harm by accessing or manipulating the neural signal information with the help of cybercrime devices and access and control the brain activities. There are two types of devices used for cybercrime activity that is (1) Deep Brain Stimulation (DBS) (2) Brain Computer Interface (BCI). These types of devices actually perform direct access to neural computation and stimulate and read the brain activities. They are generating safety and security concerns. In [21], Neurocrime refer to Specific term use for this activity is "*brain cracking*". Researcher can access user's personal information that is may be negative impact on society. It is possible the BCI device use for cybercrime because user all social and bank account

PIN number information in his/her own mind.

Computer Crime:

In [2], Computer is a rapid growing technology that are used to handle big data, banking work, buy and sell, GPS System, navigation System, use for Monitoring Heart Beat Rate, Weight Lose, Calories intake, Blood Pressure, Arithmetic Operations, Reading, Writing, Scheduling activities, Entertaining, Learning, gaming and communication. Internet also gives a huge expansion in computer and reduces distance between the information. With the increasing use of computer technologies security threats are also increase people use this technology for criminal purposes such as hacking, cracking the brain, fraud and information warfare resulting of this technology leads to cybercrime. In [7], another computer crime source is ecosystem with the use ecosystem malicious misuse should be expected. Source of ecosystem is TVs, eye-wears, Home appliances, automobiles, watches. Computer devices. According to research these devices connected to internet in 2011 is 9 billion and would be 50 billion in 2020. In [8], Computer technology also used in medical applications such as artificial cardiac pademakers and wearable heart rate monitors that are designed to accessing and processing the information. Heart beat monitor device rapidly increase so there also increase privacy and security issues like wirelessly hacking the security and privacy of the patient with low-cost devices that change the patient's therapies, disable therapies this leads to harmful for patients.

BCI Cycle:

In [9], Brain Computer Interface (BCI) are of two types Invasive and non-

invasive. Invasive BCI directly connected to central nervous system and control brain signals with electrode arrays. Whereas non-invasive BCI control brain activity through electroencephalography (EEG) and electromyography (EMG) both are neuroimaging technologies. Invasive and non-invasive technology creates a direct link between the computer and users brain through electrode. This interaction between the computer and users brain describe with 4 phases. In [10], First phase is input that generate with brain activity and when BCI user performs some mental task. For example when BCIs users control wheel chair different possible choices displayed on the interface that user is watching. Brain activity Pattern used in BCI are called event related potentials (ERPs) that measures the responses directly through sensory, cognitive, or motor event. P300 signal that are picked up by the BCI increasingly used in ERP for the process of decision making. In [2], Second phase measures the brain activity from the user's brain and convert these measure to perform certain task. In measurement phase BCI is based on electroencephalogram (EEG), Magnetoencephalography (MEG), and functional magnetic resonance imaging (fMRI). In this stage raw data or brain signal measured and decoded into well form. In third phase of the BCI cycle raw data or brain signal convert into noise free data and extract the related information from the brain signal and discard the irrelevant information like background noise because this noise disturb the mental task. In fourth phase when remove noise from signal converted into output and user can control the different devices (wheelchairs, robot, and sensor devices) with BCI applications.

BCI Technologies:

In [1], Brain Computer Interface (BCI) is a Communication system between

brain and other devices. In [11]-[13], in BCI technology we do not access brain directly to send and receive brain information instead of this we use electrophysiological signals that directly measures the neural activities. In [12], BCI technology first introduced in 1970s, that is used to overcome the needs of people in medical, non-medical, commercial, military. In medical BCIs technologies used for spinal card injuries. In [5], non-medical field BCIs technologies used in marketing, gaming, entertainment and consumer-grade BCI systems like (Emotive System [5], Neurosky [6] and g-tech medical Engineering [14]) these are all provide the low cost BCIs applications. These applications classified into mind controlled mouse and keyboard, hand free arcade games, mind controlled games. In [19], recently some researcher form Taiwan build an online system that uses electrical signal produced by skeletal muscles first 45 minutes of the game. In [17], Nielson Company developed an EEG based device in 2008 for marketing.

Privacy and Security in Neural Engineering:

In [17], present first software to get private information from user's brain by using Brain Computer Interface (BCI). In [20], main purpose of BCI's device establish the communication channel between user's brain and BCI device. Device can be collect, access the user personal information, user privacy and sensitive information on simulate device interface and "date collection and processed by BCI device is also risk factor". BCI technology allow to hacker to study the personal and mental life of user, alike personality, mode even user's social life, PIN number and ATM password etc. Researcher can be blackmail or threat the use with sensitive information. In [17], BCI get neural signal by using EEG and analyze these signals by using P300

response to get user private information like pin code, location, date of birth, banking information, ATM pin code. We need to overcome private and security issues that are generating with BCI technology.

BCIs Technologies to Extract User Private Information:

In [1], extracting private information from users in different way by hijacking and or adding or replacing the BCI components. In [18], oddball paradigms are also extract private information from users. In [19], Guilty knowledge test based on hypothesis this technique also used for extract information from user.

BCI Effect on Military:

In [22], BCI technology is use for warfare injury (fight injury). New technology use for the treatment of injures soldiers in wars of Iraq and Afghanistan. These devices use in military for improve the military performance and achieving the goals but with BCI technology we will control the brain of any person and we can perform the criminal activity through him alike threat any person a kill anyone. With BCI device increase the rate of terrorism, social threat the society. All those activities ethical risks or harm full factors for the society.

Research Question:

What is brain hacking and its ethical issues?

Brain hacking issues related to privacy and security?

BCI Technologies used in military?

Methodology:

We are download forty research papers from different scholar's sites and journals, against different keywords, fourteen are irrelevant paper for our topic, twenty six related to our topic brain hacking. We are deeply studies these paper and compare literature review from different angle, we are designs different questions like brain hacking is the way of leak privacy, source of encoding the sensitive information etc. We are already explain all other question in our previous work and summarized result. We have explained our comparison in this table.

Results:

Category	Attack	illegal Activity	Ethical Issues
Neurocrime	Affects on the brain only indirectly(e.g :limiting, modifying disrupting device function)Thinking, judgment memory	Misuse of neural devices , Terminate or disrupting functions of device	Physical harm, Manipulate neural information, moral responsibility
Computer crime	Physical and mantel harm, Telecommunication networks,	Cracking, fraud, identity theft ,financial theft, information warfare	Information security ,biological information ,private and sensitive date
Brain comput	Direct pathway	Effect on nerves	Direct access

er interface(BCI)	between user's brain and external device	system, Change the pathway of signal, reprogramming, warless hijacking	the neuronal information, Damage the mussels and nerves system, neurocrime, brain hacking
Brain hacking	Brain nerves signal, thinking ,	Password cracking, Identity theft, Phishing and fraud	PIN code break, bank, debit card digits, location, faces, personal identification, privacy, psychological issue
Privacy and security break in neural engineering	Neural security, Attack Biometric system, hijacking adding and replacing BCI components	Neural security, Brain spyware	Authentication brake by unauthentic source,
Brain Implants in the Military	With Embedded system, Control locally or globally	Brain Jacking, use extreme drugs (for brain implant)	Soldier's Behaviors, Reversibility (removable without any residual effects), Remove Decision Making of the war fighters

Future work:

- Make an army and use his own purpose control the brains of soldiers and accomplish anything which they are not want to do.
- With BCI Technology will be destroy the society is also ethical Issue.
- Terrarium accomplish with brain hacking, it is ethical issue. It is part of neurocrime.
- Destroy the social life (blackmail) of any person with cracking the brain. Is ethical issue.
- Threat to the any person financially, morally, ethically and socially with BCI Technology.

Conclusion:

This paper describes the BCI Technology and its ethical issues related with them. We discuss the tools related to BCI technology. BCI Technology improves the life of patients and also used in gaming, Entertaining, Marketing and in Military

warfare. We also examine and discuss the issues that generated with the use of BCI technology like Brain Hacking, Brain Jacking, and password cracking actually by using BCI technology security or privacy issues rise. BCI technologies have also some ethical issues related with them like pin code, location, date of birth, banking information, ATM pin code. To overcome these issues we must have some law and policy and strategies for prevention of brain hacking.

References

[1]   Bonaci, T., Calo, R., & Chizeck, H. J. (2014, May). App stores for the brain: Privacy & security in Brain-Computer Interfaces. In *Ethics in Science, Technology and Engineering, 2014 IEEE International Symposium on* (pp. 1-7). IEEE.

[2]   Ienca, M., & Haselager, P. (2016). Hacking the brain: brain–computer interfacing technology and the ethics of neurosecurity. *Ethics and Information Technology*, *18*(2), 117-129.

[3]   Young, S. (2013). Samsung demos a tablet controlled by your brain. *MIT TechnologyRev.*

[4]   Seligman, L., & Reichenberg, L. W. (2015). Theories of Counseling and Psychotherapy with My Counseling Lab with Video Enhanced.

[5]   Zioga, P., Chapman, P., Ma, M., & Pollick, F. (2014). Wireless Future: Performance Art, Interaction and the Brain-Computer Interfaces.

[6]   Martinovic, I., Davies, D., Frank, M., Perito, D., Ros, T., & Song, D. (2012, August). On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces. In *USENIX security symposium* (pp. 143-158).

[7]   Evans, D. (2011). The internet of things: How the next evolution of the internet is changing everything. *CISCO white paper*, *1*(2011), 1-11.

[8]   Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., ... & Maisel, W. H. (2008, May). Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *Security and Privacy, 2008. SP 2008. IEEE Symposium on* (pp. 129-142). IEEE.

[9]   Van Gerven, M., Farquhar, J., Schaefer, R., Vlek, R., Geuze, J., Nijholt, A., ... & Desain, P. (2009). The brain–computer interface cycle. *Journal of neural engineering*, *6*(4), 041001.

[10]   Fazel-Rezai, R., Allison, B. Z., Guger, C., Sellers, E. W., Kleih, S. C., & Kübler, A. (2012). P300 brain computer interface: current challenges and emerging trends. *Frontiers in neuroengineering*, *5*, 14.

[11]   Wolpaw, J. R., Birbaumer, N., Heetderks, W. J., McFarland, D. J., Peckham, P. H., Schalk, G., ... & Vaughan, T. M. (2000). Brain-computer interface technology: a review of the first international meeting. *IEEE transactions on*

rehabilitation engineering, *8*(2), 164-173.

[12] Wolpaw, J. R., Birbaumer, N., McFarland, D. J., Pfurtscheller, G., & Vaughan, T. M. (2002). Brain–computer interfaces for communication and control. *Clinical neurophysiology*, *113*(6), 767-791.

[13] Wolpaw, J., & Wolpaw, E. W. (2012). *Brain-computer interfaces: principles and practice*. OUP USA.

[14] Perdikis, S., Leeb, R., Williamson, J., Ramsay, A., Tavella, M., Desideri, L., ... & d R Millán, J. (2014). Clinical evaluation of BrainTree, a motor imagery hybrid BCI speller. *Journal of neural engineering*, *11*(3), 036003.

[15] Bonaci, Tamara, Ryan Calo, and Howard Jay Chizeck. "App stores for the brain: Privacy & security in Brain-Computer Interfaces." *Ethics in Science, Technology and Engineering, 2014 IEEE International Symposium on*. IEEE, 2014.

[16] Yoh, M. S., Kwon, J., & Kim, S. (2010, September). NeuroWander: a BCI game in the form of interactive fairy tale. In *Proceedings of the 12th ACM international conference adjunct papers on Ubiquitous computing-Adjunct* (pp. 389-390). ACM.

[17] Martinovic, I., Davies, D., Frank, M., Perito, D., Ros, T., & Song, D. (2012, August). On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces. In *USENIX security symposium* (pp. 143-158).

[18] Huettel, S. A., & McCarthy, G. (2004). What is odd in the oddbjall task?: Prefrontal cortex is activated by dynamic changes in response strategy. *Neuropsychologia*, *42*(3), 379-386.

[19] Wolpe, P. R., Foster, K. R., & Langleben, D. D. (2010). Emerging neurotechnologies for lie-detection: promises and perils. *The American Journal of Bioethics*, *10*(10), 40-48.

[20] Klein, E., & Ojemann, J. (2016). Informed consent in implantable BCI research: identification of research risks and recommendations for development of best practices. *Journal of neural engineering*, *13*(4), 043001.

[21] Iencaa, M. (2015). Neuroprivacy, neurosecurity and brain-hacking: Emerging issues in neural engineering. In *Bioethica Forum* (Vol. 8, No. 2, pp. 51-53). Schwabe.

[22] Kotchetkov, I. S., Hwang, B. Y., Appelboom, G., Kellner, C. P., & Connolly Jr, E. S. (2010). Brain-computer interfaces: military, neurosurgical, and ethical perspective. *Neurosurgical focus*, *28*(5), E25.