

Exploring the Feasibility to Authenticate Users of Web and Cloud Services Using a Brain-Computer Interface (BCI)

Michael Philip Orenda¹, Lalit Garg^{1,2}(✉) , and Gaurav Garg³ 

¹ University of Liverpool, Liverpool, UK
lalit.garg@um.edu.mt

² Computer Information Systems, University of Malta, Msida, Malta

³ Intelligent Systems Research Centre, University of Ulster, Coleraine, UK

Abstract. Business has come to a point whereby there is a substantial reliance on computing devices. People using machines need to be identified by who they are and not what they know or have. Real identity is the individual. Biometrics is the way to go if this is to be achieved. The biometric is a statistical measurement of biological data; be it physical, chemical or electric. Brain Computer Interface (BCI) is a maturing technology, becoming more affordable, easier to use and integrate with computing devices. With the increasing need of the internet based services (web and cloud services), it has become paramount for identification technologies to get close to natural means of identification, and biometrics offers this mechanism because it is a genuine identity of an individual. Therefore, this work aims to explore the feasibility that computer systems can use brain signals as a biometric method for authentication for web and cloud services users through a brain-computer interface (BCI). Though the main aim of this study is not to create a perfect solution, yet use the prototype as a suggestion to spur and provoke identification mechanisms to catch on in this direction. This study has been validated using the electroencephalography (EEG) scans using the Emotiv's 5-channel EEG headset and recording devices and the survey of the 52 volunteers participated in the study. As the same brain signals authentication can be used for all services irrespective of service or provider, therefore, it can be an ideal candidate for the Biometrics-as-a-Service (BaaS). The brain scan can be stored once at the BaaS provider and would be used by all service providers for all services. It can also be combined with other authentication methods to have multi-factor authentication (MFA) for improved security.

Keywords: Biometrics · Identification · Authentication · Web services
Cloud services · Brain computer interface (BCI)
Electroencephalography (EEG) · Biometrics-as-a-Service (BaaS)

1 Introduction

Humans are social beings. In this social society, each one has a need or demand and may be a supply to others. In social interactions, which have also grown to business interactions, there is need to identify each entity. The fundamental ways of identifying each

other are by sight, voice, and feel for those with disabilities. For, those with no sight disability, the face of the other human is the basic and natural way to identify the person. A human face has many features which make it almost unique (Prakash and Rogers 2015, p. 309–p. 310; Shyam and Singh 2016, p. 2; Dospinescu and Popa 2016, p. 20–p. 21). We know people by their faces, physique and voice, and through this way of identification, we interact appropriately. Business is the interaction between human beings. Identification, even in business interactions is key for appropriate interactions and in today’s business, computers have become an integral part and for this reason, computers also need to have a mechanism for identifying entities. Biometrics is a statistical measurement of the physiological and behavioural aspects of an individual. It is paramount for identification mechanisms to get as close to natural means of identification and biometrics offers this mechanism because it is the true identity of an individual. Here, the hypothesis considered to prove is “Neural signals through a Brain Computer Interface (BCI), when matured enough can be effectively used for Identity Management.”

With the ever increasing usage of the web and cloud services by humans, authentication and identity become a challenge and growing need. In this study, a prototype system is implemented to explore the feasibility that computer systems can use brain signals as a biometric method for authentication for web and cloud services users through a brain-computer interface (BCI). As the same brain signals authentication can be used for all services irrespective of service or provider, therefore, it can be an ideal candidate for the Biometrics-as-a-Service (BaaS). The brain scan can be stored once at the BaaS provider and would be used by all service providers for all services. It can also be combined with other authentication methods to have multi-factor authentication (MFA) for improved security.

Therefore, the scope of this study is to explore the feasibility of using brain signals as a way of authentication. The study does not intend to create an immediate working solution, but a suggested means of authentication using a Brain Computer Interface integrated into a web or cloud application. Web and cloud users’ anticipations, optimism towards using neural signals are also surveyed in this study.

1.1 Downsides of the Popular Authentication Methods

Username & password combination is the most commonly used and most easily implemented authentication and authorization technique used in web applications. However, there are disadvantages to this technique. One disadvantage to this technique is that it depends on the user’s cognitive ability, hence it is the security stored in the individual’s brain. Many business services; financial services, insurance services, government services, retailers, wholesalers, etc. are increasingly using the internet (web and cloud) and computing devices to trade and offer services online, where all type of user data is now being made accessible on-the-go through the cloud networking. It would mean that for each of these services offered online (through web or cloud), a person would, therefore, need to have more than one set of authentication credentials. It implies that a user should recall all the usernames and passwords for each online service (web or cloud) offered to which they have subscribed to and an increasing number of devices that connect online. (Nasirinejad and Yazdi 2012; Conklin et al. 2004).

It is like having a big bunch keys for different doors in multiple locations. Here, knowing which key unlocks which door and losing a key will not be a desirable experience.

A second drawback is that each institution offering web or cloud services has its own security policies. These differences in security policy enforcement, force users to use different credentials for each web and cloud service. Some of these policies include the number of characters, type of characters and expiry periods of the credentials. (Nasirinejad and Yazdi 2012)

Another drawback is that passwords are vulnerable to dictionary attacks. If anyone guesses the correct password or uses brute force to dig up the password, they can easily masquerade as the authorised user (Thorpe et al. 2005, p. 3)

Though the fingerprints as biometric-based authentication are becoming very popular nowadays, however, the main downside of using fingerprints is the fact that these can be stolen. It comes as a surprise that stolen fingerprint data is more than estimated by the U.S. Office of Personnel Management (Kerner 2015; Constantin 2015). One cannot change fingerprints; therefore, when stolen, nothing can be done about it because an individual cannot change his/her fingerprints. It is essential that authentication systems should allow changing authentication data in case of compromise (Thorpe et al. 2005, p. 4)

BCI technologies are not yet matured enough for a wide acceptance. However, this disadvantage will be swept away as more interest in this area of research would yield breakthroughs. O’Gorman (1996, p. 61–p. 62) also foresees that the future of biometrics could be bright given the fact that the prices and sizes of biometric devices are reducing.

1.2 Why EEG Signals?

There have been a lot of research for non-invasive observation of brain activity. In a non-invasive method, no surgery is required to place equipment for monitoring brain and neural activities in the body. These methods include functional Magnetic Resonance Imaging (fMRI), Positron Emission Tomography (PET), Transcranial Magnetic Stimulation (TMS), Near Infrared Spectroscopy (NIRS), and Electroencephalograph (EEG) or Magnetoencephalography (MEG).

The fMRI device measures by detecting oxygen supplied blood to the brain. Brain’s Neural activities are observed through bloodstream fluctuations, thus generating an fMRI activity map (Garg et al. 2013). PET beams positrons, an anti-electron of the same mass but opposite charge, to facilitate viewing of bio-chemical reactions. CT-scans use X-Ray technology with 360° rotational system to get 3D images. This technology involves radiation and should not be used frequently. NIRS is similar to fMRI but less expensive and portable. It measures brain activities using hemodynamic (Blood Oxygenation Level) response of neurons (Garg et al. 2013).

EEG is an electrophysiological signal measuring device, which measures electric activities of neurons in real-time. Voltage pulses are detected by the electrodes placed on the scalp. These recorded signals provide information about activities in the brain. (Katona and Kovari 2015). In essence, the EEG is recording and measurement of voltage fluctuations of the brain and with each brain being unique; there is a high

possibility that these voltages can be used for identification (Yang 2015, p. 10; Campisi et al. 2012). It is consequently proven that an individual can be identified using EEG signals and, additionally, EEG signals from individuals apart from identity can be used to carry out various ICT, robotic and other electronic functions (Palaniappan 2008; Yoon Jae et al. 2015).

The EEG recorded brain waves can be divided into three frequency bands; slow, moderate and fast which are categorized as; delta (<4 Hz), theta(4–7 Hz), alpha (8–15 Hz), beta(16–31 Hz) and gamma (>32 Hz) (Schultz 2012).

An advantage of EEG worth mentioning is that it does not exclude people with disabilities. Unlike the fingerprint solution to authentication when stolen, EEG authentication data can always be changed while identity is still retained. This can be done by choosing different type of cognitive activity, few of them may be left-hand push, right hand pull, right-leg up action etc. and other combinations. and recording the corresponding EEG/electrophysiological signal in the database for matching and authorization purpose at later stage. Also, these recordings are unique to every individual.

fMRI and PET produce high resolution images. However, these images are large in size and thus expensive and slow to process. They are primarily used for medical examinations. TMS could raise some controversy because the effect of depolarization is not known. EEG devices being relatively inexpensive and portable have become more available in the market, which will bring into play more innovations from many researchers, businesses and developers beyond medical use. (Katona and Kovari 2015) There are many uses of EEG device, especially in the gaming and toy industries, where action and control are detected from brain signals.

2 Methodology

A biometric fingerprint reader is used to capture fingerprints for use in authentication. Likewise, the fact that there is already an interface that is developed to send neural signals from the brain to a computer system, the Brain Computer Interface (BCI) can be used to capture brain signals that may well be used for authorization and authentication amongst other uses. It is logical to create systems that use EEG as there is an interest to research more in the area of EEG. (Al-Hudhud 2014).

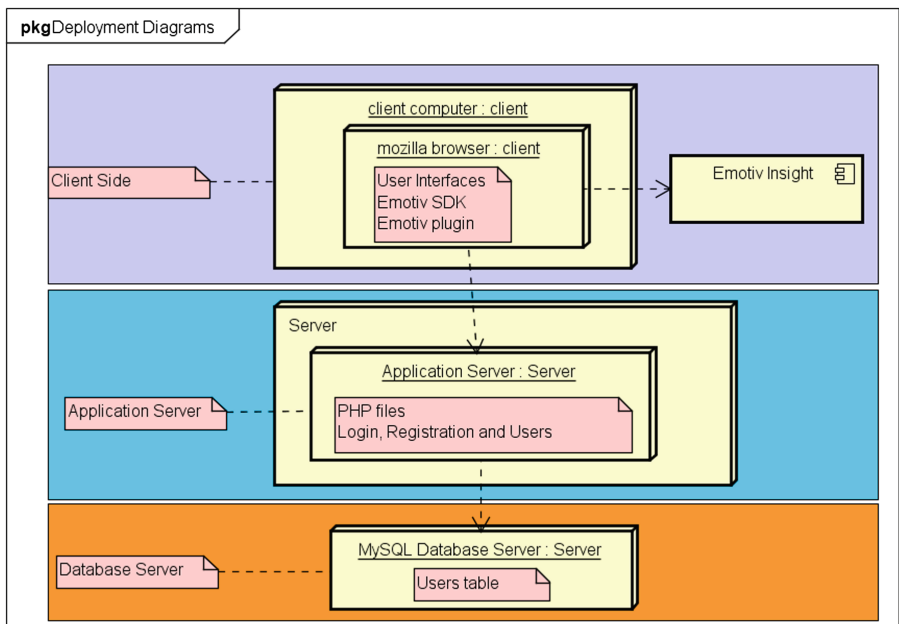
In theory and practice, authenticating web and cloud services users using brain signals should not be a complex undertaking. Research carried out by Novak and Švogor (2016) indicates the use and growth of Component-based systems or designs (CBD) for web and cloud services. Computer systems are components working together to achieve certain objectives. These components are both hardware and software components. CBD simplifies innovations and allows for independent improvements and reuse of each component (Sommerville 2011, p. 452–p. 478). Using components help us apply the design pattern and principle of separation of concerns (SoC) that makes it possible for independent research and improvements on each component. It means that research on EEG hardware and EEG software can independently continue. Improvement of current computer hardware, and software

(browsers, thin client and desktop software), and programming languages can also independently improve to include EEG effortlessly.

The prototype, along these lines, is a three-tier architecture with each tier having subcomponents. The main subcomponent of this feasibility study is the BCI which resides at the client-side of the architecture.

2.1 System Architecture and Components

The prototype system is made up of server side and client side devices as well as software. The server side is essentially a computer that has a web server, application server and database server. Client side consists of a computer that has a web browser such as Mozilla's Firefox Browser which, when browsing the web application will pull the client-side script and prompt a download of a plugin from Emotiv. The client side also includes the Emotive Insight, a Brain-Computer Interface device from Emotiv. All components, except the components specific to the Emotiv Insight, are common components. Figure 1 illustrates the components and architecture of the prototype.



powered by Astah

Fig. 1. System Architecture & Components

2.2 Emotive Insight Brainwear

Emotive Insight Brainwear (say Insight hereafter), as shown in Fig. 2, is a five channel EEG headset that records brainwaves and make those brain signals available for further



Fig. 2. Emotiv Insight Brainwear (Emotiv 2 2016)

processing. Insight connects to a wide variety of computing devices; computers, tablets and phones with support for the common operating systems; Windows, Linux, MAC OSX, Android and IOS via Bluetooth. The five signal channels are AF3, AF4, T7, T8 and Pz. (Emotiv 2016)

2.3 Emotiv Plugin and SDK

The Emotiv software development kit (SDK) used for this project consists of mainly these four JavaScript files; `EdkDll.js`, `EmoState.js`, `EmoEngine.js` and `ElsCloud.js`. This SDK communicates through a plug-in software, `EmotivBTLE.msi` (Emotiv 2016), installed in the operating system and used by the browser to connect to the Insight. Web pages in the prototype that require a connection to Insight will have to include the plug-in object that connects to the device. The plug-in object is embedded in the HTML using the code

```
<object id="plugin0" type="application/x-
  emotivlifesciencesbtle" width="0" height="0">
  <param name="onload" value="pluginLoaded" />
</object>
```

Emotiv provides a list of references on their website (`Cpanel.emotivinsight.com` 2016) which, depending on the requirements are used in JavaScript files. The provided SDK is primarily event-based. Hence, the page has to be programmed as well to respond to the events originating from users and the events from Insight.

2.4 Implementation

Code for authenticating using mental commands is written in PHP. The comparison is not clear-cut as with a normal password comparison from a database compared to the provided one. Emotive insight records the electrical activity of brain and saves it in the comma separated value (*.csv) format. Emotiv Insight data is comma delimited with some values repeating (see Table 1). The code takes the highest repeated value from Emotive Insight data in the database and compares to the highest repeated value provided by the user through the login page.

Table 1. Illustration of the user database including part of Emotiv Insight recorded EEG data

Column	Data
usr_id	21
username	Michael
firstname	Michael
lastname	Orenda
email	michael.orenda@online.liverpool.ac.uk
EEG of 'neutral' state brain	<... ..> ... "4174.358872", "4174.358872", "4174.358872", "3848.717855", "3868.205034", "3865.128111", "3861.025547", "3861.025547", "3856.410162", "3850.769137", "3850.256316", "3860.512726", "3864.61529", "3851.281957", "3845.640932", "3860.512726", "3857.435803", "3854.35888", "3872.307598", "3963.589647", "3941.025545", "3957.948621", "3982.564005", "3973.333236", "3948.717852", "3954.871698", "3970.769134", "3961.025544"... ..>
EEG of 'push' command	<... ..>
EEG of 'pull' command	<... ..>
EEG of 'up' command	<... ..>
EEG of 'down' command	<... ..>
EEG of 'left' command	<... ..>
EEG of 'right' command	<... ..>

The registration and login at the user interfaces (page) do not have the usual submit button. Fields are event-based, hence the user of the client-side scripting (JavaScript). With a click being an event for the mental command fields, each click triggers an event that connects to Emotiv Insight which also responds. Emotiv Insight responses are also events that are captured and necessary action taken. All successful actions trigger a database transaction, to either save data if the page is registration page or authenticate if the page is the login page.

2.5 Web Page for Biometric Authentication Using Brain Signals

Connection Testing Webpage.

It is a webpage that is used to ensure that there is a connection to Insight headset. Emotiv provided the page, and there are no changes done to this webpage.

Registration and Login Page.

It is a page created to allow users to record their mental commands into the system (see Fig. 3(a)). The page has some changes but relies on the samples obtained from Emotiv as examples. The page has input fields where a user can enter their username, first name, last name and email. The other fields are event based fields, whereby the user clicks on the mental command which he/she wants to train. It is paramount to train the neutral state of the brain first. Successful and accepted recordings are saved into the database using Ajax. There is no submit button, the acceptance of the recording is the event equal to 'submit' in this set-up.

The login page is similar to the registration page. It only differs because the user will only enter a username and select the mental command he/she wish to login with (see Fig. 3(b)).

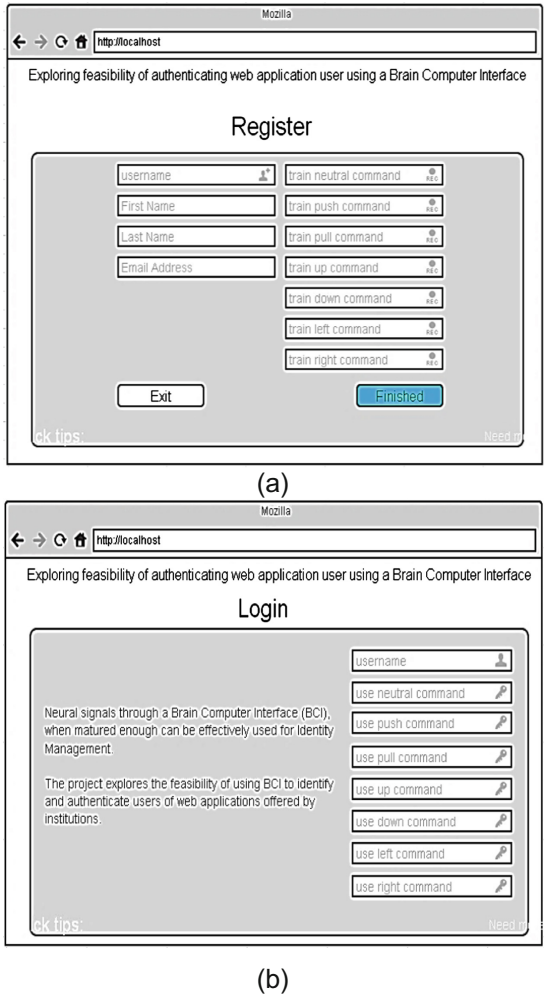


Fig. 3. (a) Registration Page and (b) Login Page

2.6 Application Server and Database

The application server consists of Apache v2.4 and PHP v5.4. For installation of these servers, Xampp and WAMP both were tested to get the complexity of the configurations out of the way. Xampp and WAMP both configure Apache to run PHP scripts which are used at the back end, more importantly, to communicate with the database server and holds the authentication algorithm.

The system uses MySQL database v5.6. Only one schema with one table used for authentication. In this, all the columns are considered as described on the login page. Though, other columns are optional and can be changed to some other complex brain-based command, except `usr_id` and `username` columns, which also have the UNIQUE constraint to them.

2.7 Evaluation Survey Design

A questionnaire is aimed at getting information and opinion from users. The target sample size of 52 is drawn from banks, health insurance, government, private investigation and ICT companies. The banks include the two largest banks in the region, Equity Bank, Kenya Commercial Bank and another bank CFC Stanbic and any other that will randomly accept. Health and Insurance include again the largest players in the region; Jubilee and CIC insurance. From government, targeted participants are from Kenya Revenue Authority and National Transport and Safety Authority. ICT companies included Oracle Kenya, Institute of Software Technologies, and Software Technologies Ltd. All these organisations serve millions of Kenyans thus evaluation is designed to get opinions from the wide variety of users.

A survey is done after the completion of the implementation of the prototype. The target sample size is 52 who answered the questionnaire after voluntarily interacting with the prototype. The questionnaire is designed to explore the opinion and anticipation of participants about the feasibility of using brain signals as a way of authenticating users of web or cloud services and receiving government services online and opinions about the methods and technologies used for authentication.

3 Results and Evaluation

The hypothesis tests positive if the users affirm the fact that they believe it better and will be possible to use neural signals especially brain signals for authentication.

Based on those above though rudimentary BCI prototype and survey results, it can be considered feasible to use brain signals for authentication of web and cloud based applications. The findings of the survey are better represented in a straightforward way rather than the complex percentage among the user opinion. Most of the respondents after just seeing the BCI despite knowing the difficulties, agreed that brain signals should be one of the authentication methods in the future.

Authentication Preferences and Feasibility of Using Brain Signals.

Users of this system were asked if the available authentication technologies are matured what authentication method would be their preference, 88% of the participants with $\pm 9\%$ confidence interval (c.i.) at 95% confidence level (c.l.) preferred biometrics. And 58% of these (i.e., 51% of all participants with $\pm 14\%$ c.i. at 95% c.l. specify brain signals (cf. Fig. 4). Over 80% of the participants (with $\pm 11\%$ c.i. at 95% c.l. affirmed that biometrics is the true identity of an individual.

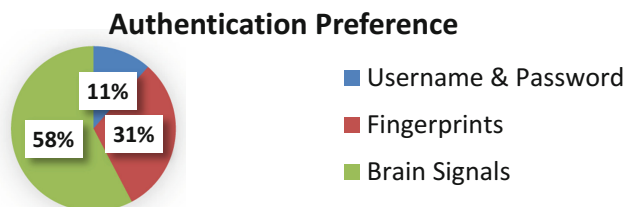


Fig. 4. Authentication Preference

Limitations of Using Brain Signals for Authentication.

Regardless of the preference for BCI-based authentication as has been experienced by the users during the registration process, it is not easy thinking for 8 s without wavering into other thoughts. Thinking left, push, pull, top, down or right is not as easy as said. Another limitation is ‘slow to use’. The device must be worn on the head, and one must ensure that there are signals being acquired. It means that it cannot be spontaneously used.

4 Conclusion

The BCI system prototype in the project is based on the Emotiv’s device, SDK and plugin (Emotiv 2016; Emotiv 2 2016; Cpanel.emotivinsight.com 2016). However, it is not worth making recommendations based on Emotiv proprietary products, but use it as a pointer to make recommendations for standardisation that would lead easy and wide usage of biometrics especially neural signals for authentication and identity management. Businesses need to identify the entities receiving their web or cloud based services or products. This basic reality of identifying entities, put to work in devices using biometrics, would prove to be a great and necessary business exploit; it could be a significant application that is required virtually in most of the electronic devices which require authentication.

This study can be further developed to perfection for use not only in internet based usage but also to other required authentication purposes in all kinds of wearable electronic gadgets which have even wider and deeper reach to users. Security systems such as opening doors and approving transactions may also be put into the context of this. Also, as we do not require the complete brain scan for the authentication, but a part of it is sufficient, the complete brain scan data can be stored in a cloud, and a part can randomly be selected for the authentication each time. During the authentication, only the selected part of the brain signal will be collected from the user and authentication process would take place in the cloud or server. If the service requires authentication process to be completed on the client side, only the selected part of the brain scan can be accessed from the cloud by the client application. It will help ensure enhanced security, faster authentication and protecting brain scans from being copied by the eavesdroppers and con-artists. Further, as the same brain signals authentication can be used for all services irrespective of service or provider, therefore, it can be an ideal candidate for the BaaS. The brain scan can be stored once at the BaaS provider and would be used by all service providers for all services. It can also be combined with other authentication methods to have multi-factor authentication (MFA) for improved security.

References

- Al-Hudhud, G., Alzamel, M., Alattas, E., Alwabil, A.: Using brain signals patterns for biometric identity verification systems. *Comput. Hum. Behav.* **31**, 224–229 (2014)
- Campisi, P., La Rocca, D., Scarano, G.: EEG for automatic person recognition. *Computer* **45**(7), 87–89 (2012)

- Conklin, A., Dietrich, G., Walz, D.: Password-based authentication: a system perspective. In: Proceedings of the 37th Annual Hawaii International Conference on System Sciences, p. 10 (2004)
- Constantin, L.: US govt's OPM underestimated the number of stolen fingerprints by 4.5 million, Cio (13284045), p. 1 (2015)
- Cpanel.emotivinsight.com.: API Reference, <https://cpanel.emotivinsight.com/BTLE-/api.htm>. Accessed 24 Sep 2016
- Dospinescu, O., Popa, I.: Face detection and face recognition in android mobile applications. *Informatica Economica* **20**(1), 20–28 (2016). Business Source Complete
- Emotiv.: About Emotiv, <http://emotiv.com/about-emotiv/>. Accessed 25 June 2016
- Emotiv 2.: Image of Emotive Insight Brainwear, <https://i1.wp.com/www.emotiv.com/wp-content/uploads/2016/04/emotiv-insight-square-w.jpg>. Accessed 26 Sep 2016
- Garg, G., Prasad, G., Coyle, D.: Gaussian Mixture Model-based noise reduction in resting state fMRI data. *J. Neurosci. Methods* **215**(1), 71–77 (2013)
- Kerner, S.M.: OPM says far more fingerprint data stolen than first reported. *Eweek*, 1 (2015). Business Source Complete
- Katona, J., Kovari, A.: EEG-based computer control interface for brain-machine interaction. *Int. J. Online Eng.* **11**(6), 43–48 (2015). Computers & Applied Sciences Complete
- Nasirinejad, M., Yazdi, A.: SASy username and password management on the cloud. In: Proceedings 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic, CyberSec 2012, pp. 242–246 (2012)
- Novak, M., Švogor, I.: Current usage of component based principles for developing web applications with frameworks: a literature review. *Interdisc. Description Complex Syst.* **14**(2), 253–276 (2016)
- O’Gorman, L.: Fingerprint verification. In: Jain, A.K., Bolle, R., Pankanti, S. (eds.) *Biometrics*, pp. 43–64. Springer, Boston (1996)
- Palaniappan, R.: Two-stage biometric authentication method using thought activity brain waves. *Int. J. Neural Syst.* **18**(01), 59–66 (2008)
- Prakash, A., Rogers, W.: Why some humanoid faces are perceived more positively than others: effects of human-likeness and task. *Int. J. Soc. Robot.* **7**(2), 309–331 (2015). PsycINFO
- Schultz, T.L.: Technical tips: mri compatible eeg electrodes: advantages, disadvantages, and financial feasibility in a clinical setting. *Neurodiagnostic J.* **52**(1), 69–81 (2012)
- Shyam, R., Singh, Y.: Multialgorithmic frameworks for human face recognition. *J. Electr. Comput. Eng.*, 1–9 (2016). Academic Search Complete
- Sommerville, I.: *Software Engineering*, pp. 452–478. Pearson, Boston (2011)
- Thorpe, J., Van Oorschot, P., Somayaji, A.: Pass-thoughts. In: Proceedings of the 2005 Workshop on New Security Paradigms - NSPW 2005 (2005)
- Yang, S.: The use of EEG signals for biometric person recognition, Doctoral dissertation, University of Kent (2015)
- Yoon Jae, K., Sung Woo, P., Hong Gi, Y., Moon Suk, B., June Sic, K., Chun Kee, C., Sungwan, K.: A study on a robot arm driven by three-dimensional trajectories predicted from non-invasive neural signals. *Biomed. Eng. Online* **14**(1), 1–19 (2015)