Paper Title	**Personalizing Health and Food Advices by Semantic Enrichment of Multilingual Cross-Domain Questions**
Authors	Tarek Helmy, Ahmed Al-Nazer (King Fahd University of Petroleum and Minerals, Dhahran, KSA)
Conf. or Journal Name	International GCC IEEE 8th Conference and Exhibition (GCCCE), Muscat, pp. 1 – 6, 1-4 Feb. 2015.
Abstract	Web search engines help in retrieving the scattered information from the Web, albeit with a number of limitations. They can't understand or enrich the user's natural language questions easily or offer the recommendation that fits the user's exact needs. Health and food information are examples of critical domains where the users have a lot of questions that need to be understood well, enriched and processed to retrieve answers that match the user's needs. Using the personalization and the semantic techniques help us to propose a framework that enriches the user's questions and retrieves more relevant results. In this paper, we analyze the user's preferences related to the health and food domains, and then propose a user's profile ontology that represents these preferences and map them to the pre-defined domain ontologies. The proposed framework has been implemented and the experimental results show promising results with user satisfaction.
Keywords	***Web Search Engines, Natural Language, Personalization, Semantic Techniques, Ontologies***

Paper Title	**Performance Evaluation of System Resources Utilization with Sandboxing Applications**
Authors	Tarek Helmy, Ismail Keshta, Abdallah Rashed (King Fahd University of Petroleum and Minerals, Dhahran, KSA)
Conf. or Journal Name	Lecture Notes in Electrical Engineering, Information Science and Applications, Springer Berlin Heidelberg, vol. 339, pp 475-48, 2015.
Abstract	Sandboxing is a popular technique that is used for safely executing untested code or testing un-trusted programs inside a secure environment. It can be employed at the operating system level or at the application level. In addition, it limits the level of access requested by the untested programs in the operating system by running them inside a secure environment. Therefore, any malicious or improperly coded programs that are aiming to damage hardware or software recourses will be prevented by the sandboxing. In this paper, we want to assess the effect of sandboxing on the system's recourses utilization. We will examine and evaluate the operating system performance with Sandboxie, Bufferzone and Returnil sandboxes applications. Different performance parameters are considered, such as the execution time by the CPU for each sandbox and the read/write speed for various input output devices like memory and disks. Moreover, it is important to highlight that we have evaluated the mentioned sandboxing applications under the effect of having a virus that is attacking the operating system. We defined our own performance metrics that contain the most important parameters used in evaluating the related research work.
Keywords	***Sandboxing , Bufferzone, Returnil, Untested Code, Operating System, System's Recourses Utilization***